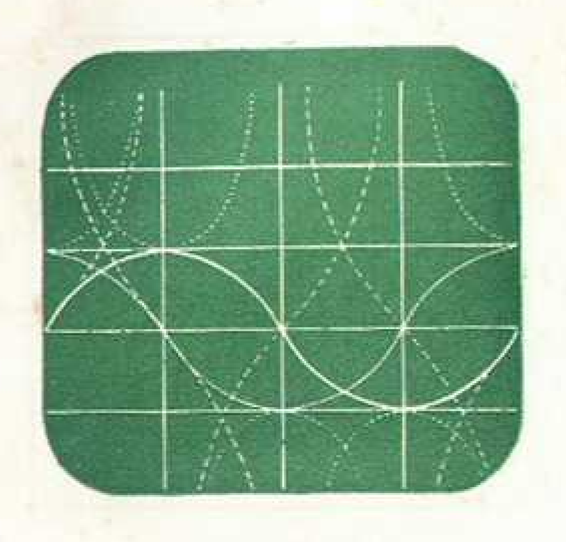


单 墫　余红兵

不定方程

上海教育出版社

(沪)新登字107号

不定方程

单墫 余红兵

上海教育出版社出版发行
(上海永福路123号)
各地新华书店经销　　上海崇明印刷厂印刷
开本 787×1092 1/32 印张 5 字数 108,000
1991年9月第1版 1991年9月第1次印刷
印数 1—3,000 本
ISBN 7-5320-2350-8/G·2285　　定价：1.70元

前　言

不定方程肇源极古，我国古代算书《周髀算经》中已记载着"勾三股四弦五"的结论，这实际上给出了三元二次不定方程 $x^2+y^2=z^2$ 的一组整数解．一千七百多年前的古希腊数学家丢番图(Diophantus)对不定方程作过很多研究，因此，不定方程也称为丢番图方程．

随着数学的不断发展，不定方程的重要性日益显著．现代数学的重要分支，如代数数论，代数几何，表示理论……都在这里交汇．不定方程几乎成为一块试金石，用以检验新的数学理论和新的数学方法．

本书是为丰富中学生的数学知识而写的小册子．为便于学生学习，尽量使用初等方法来讨论在初等数学(特别是各级数学竞赛)中经常遇到的不定方程．学生阅读不定方程所需的一些整数知识，在本书的附录中也作了阐述，可供参考．

作　者

目　录

一、一次不定方程

考虑一个古老的问题：

笼子中装有若干只三脚怪兽和山羊，共有23只脚，如果怪兽多于一只，问其中有多少只脚是怪兽的？

设x为笼子中的怪兽数，y为山羊数，则有

$$3x+4y=23. \quad ①$$

很明显，这个二元一次方程有无限多组实数解．但这里要求x和y都是正整数．

方程①的正整数解可以用尝试法来求，先将①变形为

$$x=\frac{23-4y}{3}.$$

由于x和y必须是正整数，而当$y>5$时，x为负数，所以$y\leqslant 5$．令$y=1, 2, 3, 4, 5$，并算出相应的x值：

y:	1	2	3	4	5
x:	$\frac{19}{3}$	5	$\frac{11}{3}$	$\frac{7}{3}$	1

因此，方程①有两组正整数解：$x=5, y=2$及$x=1, y=5$．但原问题中指明笼中怪兽多于一只，所以怪兽有5只，从而有15只脚是怪兽的．

像①这样的方程（组），未知数的个数多于方程的个数，而解的取值范围有某种限制（如必须为有理数、整数、正整数等），就称为不定方程（组）．

如无特别申明，本书中字母均代表整数．并且，我们只讨

论不定方程的整数解.

本节,我们先讨论二元一次不定方程

$$ax+by=c, \qquad ②$$

其中 a, b, c 都是已知的整数,且 a, b 不全为 0.

方程 ② 显然有无穷多组实数解. 它甚至有无穷多组有理数解, 因为(不妨设 $b\neq 0$) x 可任取一个有理数值 r, 解出 $y=\frac{c-ar}{b}$, 也是有理数.

但方程 ② 不一定有整数解.

例 1 不定方程

$$10x-15y=48$$

没有整数解.

证明 用反证法. 假设方程有一组整数解 $x=x_0$, $y=y_0$, 则有

$$10x_0-15y_0=48,$$

即

$$5(2x_0-3y_0)=48.$$

上式左端能被 5 整除, 但右边不能. 这就导出矛盾.

论证的关键是 10 和 15 的最大公约数 5, 不能整除方程的常数项 48. 由此可见, 方程 ② 有整数解的必要条件是 a, b 的最大公约数整除 c, 即 $(a, b)|c$ (于是, 如果读者愿意的话, 可以随手写出许多没有整数解的二元一次方程).

条件 $(a, b)|c$ 也是充分的, 这就是下面的定理 1. 它是不定方程中最基本的结论.

定理 1 设 a, b, c 都是整数, 且 a, b 不全为 0, 则不定方程

$$ax+by=c \qquad ②$$

有整数解的充分必要条件是 $(a, b)|c$.

证明　考虑集合

$$S=\{ax+by \mid x, y \text{ 是任意整数}\}.$$

这样，方程有整数解的充分必要条件是 $c\in S$.

请注意集合 S 的元素全是整数，并且有两个简单的性质：

(i) 如果 $m, n\in S$，则 $m\pm n\in S$；

(ii) 如果 $m\in S$，k 是任意整数，则 $km\in S$.

因为 $m, n\in S$，则有整数 x_1, y_1, x_2, y_2，使得

$$m=ax_1+by_1,\ n=ax_2+by_2,$$

从而
$$m\pm n=a(x_1\pm x_2)+b(y_1\pm y_2)\in S.$$

类似地可以证明性质(ii).

S 中有正整数（例如 $|a|$，$|b|$ 都在 S 中）. 设 d 是 S 中的最小正整数. 我们证明 S 中所有的数都是 d 的倍数.

对任意的 $m\in S$，由带余除法可知存在整数 q, r，使

$$m=dq+r,\ 0\leqslant r<d.$$

由 $d\in S$ 及性质(ii)知 $dq\in S$. 又 $m\in S$，再由性质(i)得出 $r=m-dq\in S$. 但 $0\leqslant r<d$，d 是 S 中的最小正数，所以 $r=0$ 即 $m=qd$.

特别地，$a, b\in S$ 都是 d 的倍数，因而 d 是 a, b 的公因数，$d\mid(a, b)$.

下面证明 $d=(a, b)$. 由于 $d\in S$，所以存在整数 x, y 使得

$$d=ax+by.$$

但 $(a, b)\mid a$，$(a, b)\mid b$，因而 $(a, b)\mid d$，所以 $d=(a, b)$.

S 中的数都是 (a, b) 的倍数. 由(ii)，(a, b) 的倍数也都在 S 中. 所以，S 就是 (a, b) 的倍数所成的集合.

我们已经说过，方程 ② 有整数解的充分必要条件是 $c\in$

S. 这结论就等价于$(a, b)|c$. 证毕

例 2 判断不定方程

$$51x+45y=357$$

是否有整数解.

解 为求出$(51, 45)$，我们将 51 和 45 作素因数分解:

$$51=3\times 17,\ 45=3^2\times 5.$$

因此$(51, 45)=3$. 显然 $3|357$，由定理 1 可知方程有整数解.

例 3 证明不定方程

$$ax+by=(a, b) \quad ③$$

有整数解，其中 a, b 是不全为 0 的整数.

证明 由于$(a, b)|(a, b)$，由定理 1，方程 ③ 有整数解.

③ 就是著名的裴蜀(Bézout)恒等式. 特别地，在整数 a, b 互素即$(a, b)=1$ 时，有整数 x, y 使得

$$ax+by=1. \quad ④$$

③ 及 ④ 在数论中用处甚多.

注: 当方程②有整数解时，可以假设$(a, b)=1$. 因为由定理 1，这时$(a, b)|c$，将②两边同除以(a, b)就化为同解方程

$$\frac{a}{(a,b)}x+\frac{b}{(a,b)}y=\frac{c}{(a,b)},$$

而 $\frac{a}{(a,b)}$ 与 $\frac{b}{(a,b)}$ 互素. 这在研究方程②的一般理论时经常用到.

定理 1 虽然给出了判别 ② 是否有整数解的法则，但并未告诉我们在有解时怎样实际地求出解来. 这件事将在下面解决.

当$|a|$, $|b|$都不太大时，尝试法是可行的.

例4 判断方程

$$7x+15y=1989 \quad ⑤$$

是否有整数解．如果有，试求出一组解．

解 因为$(7, 15)=1$整除1989．由定理1可知方程有整数解．为求⑤的一组解，可以先求

$$7x+15y=1 \quad ⑥$$

的一组整数解．不难看出$x=-2$，$y=1$适合方程⑥．所以$x=-2\times1989$，$y=1989$是方程⑤的一组整数解．

从定理1已经看到，方程②的求解与(a, b)有密切的关系．求(a, b)的一种方法是将a、b分解（如例2）．但一个大整数的素因数分解并非易事（试分解$2^{101}-1$）．另一种求(a, b)的方法是欧几里得算法（辗转相除法）．它的优点之一是顺便给出了②的求解方法．

欧几里得算法 设a，b都是整数，$b>0$，则按下述方式反复作带余除法，余数的值严格递降，有限步后余数必为0．

用b除a，

$$a=bq_0+r_0,\ 0<r_0<b,$$

用r_0除b，

$$b=r_0q_1+r_1,\ 0<r_1<r_0,$$

用r_1除r_0，

$$r_0=r_1q_2+r_2,\ 0<r_2<r_1,$$

………

用r_{n-1}除r_{n-2}，

$$r_{n-2}=r_{n-1}q_n+r_n,\ 0<r_n<r_{n-1},$$

用r_n除r_{n-1}，

$$r_{n-1}=r_nq_{n+1}.$$

作最后一步除法后，余数为0．这时$(a, b)=r_n$．

例5　判断方程

$$5767x+4453y=-1679 \qquad ⑦$$

是否有整数解.

解　将5767及4453作标准分解并不容易．为了求(5767, 4453)，我们作欧氏算法如下(请对照上面的一般形式，取$a=5767$，$b=4453$)：

$$5767=4453\times1+1314,$$
$$4453=1314\times3+511,$$
$$1314=511\times2+292,$$
$$511=292\times1+219,$$
$$292=219\times1+73,$$
$$219=73\times3.$$

所以(5767, 4453)=73．不难验证(作除法)$1679=73\times23$，即$73\mid1679$，由定理1可知方程(7)有整数解.

欧氏算法不仅是求(a, b)的实用方法，实际上我们还能借助它来求得方程

$$ax+by=(a, b) \qquad ③$$

的一组整数解．请注意，有了③的一组整数解(x, y)，便立刻得出②的一组解$\left(\frac{c}{(a,b)}x, \frac{c}{(a,b)}y\right)$．这样，我们顺便又给了定理1中充分性的另一种证法，这证法是构造性的．求③的一组解的具体做法是将前面说的欧氏算法倒推回去：

由算法中的倒数第二行，得到

$$(a, b)=r_n=r_{n-2}-r_{n-1}q_n,$$

这就将(a, b)表示成r_{n-2}，r_{n-1}的整系数的线性组合．用算法中在其前面的一行

$$r_{n-3}=r_{n-2}q_{n-1}+r_{n-1}$$

代入上式，消去 r_{n-1}，得

$$(a, b)=r_{n-2}-(r_{n-3}-r_{n-2}q_{n-1})q_n$$
$$=r_{n-2}(1+q_{n-1}q_n)-r_{n-3}q_n.$$

再用
$$r_{n-4}=r_{n-3}q_{n-2}+r_{n-2}$$
代入，消去 r_{n-2}，得

$$(a, b)=r_{n-3}\times\text{整数}+r_{n-4}\times\text{整数},$$

继续做下去，便求得整数 x, y，使

$$ax+by=(a, b).$$

我们看一个用倒推法求③的一组解的具体例子.

例 6 求出方程

$$5767x+4453y=-1679 \qquad ⑧$$

的一组整数解.

解 应用例 5 中的欧氏算法，将算法倒推回去，有

$$\begin{aligned}73&=292-219\times1=292-(511-292\times1)\\&=2\times292-511=2\times(1314-511\times2)-511\\&=2\times1314-5\times511=2\times1314-5\times(4453-1314\times3)\\&=17\times1314-5\times4453\\&=17\times(5767-4453\times1)-5\times4453\\&=17\times5767-22\times4453.\end{aligned}$$

因此，$x=17$, $y=-22$ 是方程

$$5767x+4453y=73$$

的一组整数解. 从而方程⑧有一组整数解 $x=17\times\left(\frac{-1679}{73}\right)=-391$, $y=-22\times\left(\frac{-1679}{73}\right)=506$.

例 7 判断方程

$$107x+73y=230 \qquad ⑨$$

是否有整数解. 如有，试求出一组解.

解　如果看出 107 及 73 都是素数(从而它们互素)，便立即得知方程有整数解．我们也可以作欧氏算法：

$$107=73\times1+34,$$
$$73=34\times2+5,$$
$$34=5\times6+4,$$
$$5=4\times1+1,$$
$$4=1\times4.$$

因此 $(107,\ 73)=1$．所以方程 ⑨ 有整数解．要求得一组解，可以像例 6 那样地进行．但列成下面的表格，则更为方便：

表中的第二行为各次带余除法所得的商(最后一次的商 4 不放入表中)．

n	-1	0	1	2	3	4
q_{n-1}			1	2	6	1
x_n	1	0	1	2	13	15
y_n	0	1	1	3	19	22

第一、二列是固定的．第三行的其他数由递推公式

$$x_n=q_{n-1}x_{n-1}+x_{n-2}$$

算出．第四行由公式

$$y_n=q_{n-1}y_{n-1}+y_{n-2}$$

算出．最后得到

$$x_4=15,\ y_4=22,$$

则
$$x=(-1)^{4-1}x_4,\ y=(-1)^4y_4.$$

即 $x=-15$, $x=22$ 是方程

$$107x+73y=1$$

的一组解，于是 $x=-15\times230$, $y=22\times230$ 是方程 ⑨ 的一

组整数解.

我们再用上面的方法求例 6 中方程

$$5767x+4453y=73$$

的一组解. 由例 5 中的欧氏算法得出表格:

n	-1	0	1	2	3	4	5
q_{n-1}			1	3	2	1	1
x_n	1	0	1	3	7	10	17
y_n	0	1	1	4	9	13	22

所以 $x_5=17$, $y_5=22$, 则 $x=(-1)^{5-1}x_5=17$, $y=(-1)^5 y_5=-22$ 是所求的一组解.

我们已建立了判别方程 ② 是否有解的法则,并且在有解时能够实际地求得一组解(这组解通常称为 ② 的特解). 然而这仅仅走了第一步. 一般说来, 考虑不定方程有下述三个步骤(请注意,问题的难度随之而增):

(i) 判断方程是否有整数解. 如果有,求出一组解.

(ii) 判别方程是否有无穷多组整数解.

(iii) 求出方程的全部整数解.

方程 ② 如果有解,是否一定有无穷多组解呢? 答案是肯定的. 因为设 $x=x_0$, $y=y_0$ 是 ② 的一组解, 则 $x=x_0+bt$, $y=y_0-at$ (t 是任意整数)都是 ② 的整数解(请读者自己代入验证). 要求出 ② 的全部整数解也并不困难. 这时我们可以设 $(a, b)=1$ 来讨论(见第 4 页的注).

定理 2 设 $(a, b)=1$, $x=x_0$, $y=y_0$ 是方程

$$ax+by=c \qquad ②$$

的一组解(特解),则其全部整数解(通解)为

$$\begin{cases} x = x_0 + bt, \\ y = y_0 - at. \end{cases} \qquad ⑩$$

这里 t 是任意整数. ⑩ 一般称为方程 ② 的通解公式.

证明　上面已经说过, ⑩ 式给出的 x, y 都是 ② 的解, 所以只要证明 ② 的任意一组整数解都可写成 ⑩ 的形式. 设 (x', y') 是 ② 的一组解, 则

$$ax' + by' = c.$$

再由

$$ax_0 + by_0 = c,$$

两式相减得

$$a(x_0 - x') + b(y_0 - y') = 0, \qquad ⑪$$

由此

$$a \mid b(y_0 - y').$$

但 $(a, b) = 1$, 故 $a \mid (y_0 - y')$. 于是有

$$y_0 - y' = at,$$

其中 t 为整数, 即

$$y' = y_0 - at.$$

代入 ⑪式, 得 $x' = x_0 + bt$. 证毕.

当 $(a, b) > 1$ 时, 如方程 ② 有整数解, 则其全部整数解为

$$\begin{cases} x = x_0 + \dfrac{b}{(a, b)} t, \\ y = y_0 - \dfrac{a}{(a, b)} t. \end{cases}$$

这里 (x_0, y_0) 是 ② 的特解, t 是任意整数.

由公式 ⑩ 不难看出, 方程 ② 的整数解 x, y 分别组成公差为 b 及 $-a$ 的等差数列. 对于 ② 的两组不同特解, 相应的通解表达式 ⑩ 的形式虽不完全一样, 但由此得出的 ② 的解集是相同的.

例 8　求出不定方程

$$321x + 219y = 690 \qquad ⑫$$

的全部整数解．

解　易见 $321=3\times107$，$219=3\times73$，从而 $(321,219)=3$（如果看不出这些，可以用欧氏算法来做）．又 $690=3\times230$，即 $3\mid690$，故方程 ⑫ 有整数解．将方程两边同除以 3，化成同解的方程

$$107x+73y=230, \tag{⑨}$$

由例 7，求得 ⑨ 的特解为 $(-15\times230,\ 22\times230)$．因方程 ⑨ 中 x 和 y 的系数互素，故可以应用定理 2，得出方程 ⑫ 的通解是

$$\begin{cases}x=-15\times230+73t,\\ y=22\times230-107t,\end{cases}$$

其中 t 为任意整数．

现在我们进一步来考虑方程 ② 的非负整数解（如果它有整数解的话），这时可假设 $(a,\ b)=1$．由定理 2，这个问题等价于确定整数 t 使得不等式组

$$\begin{cases}x_0+bt\geqslant0,\\ y_0-at\geqslant0\end{cases}$$

成立．这里，$(x_0,\ y_0)$ 是 ② 的特解．

例 9　求出方程

$$3x+5y=101 \tag{⑬}$$

的全部非负整数解．

解　我们需要求出该方程的全部整数解（注意方程中 x 及 y 的系数是互素的）．为此先求

$$3x+5y=1$$

的一组解．不难看出可取 $x=2$，$y=-1$．从而 $x=2\times101$，$y=-101$ 是方程 ⑬ 的特解．由定理 2，其全部整数解为

$$\begin{cases} x=202+5t, \\ y=-101-3t. \end{cases} \quad ⑭$$

其中 t 是任意整数．由

$$\begin{cases} 202+5t\geqslant 0, \\ -101-3t\geqslant 0 \end{cases}$$

易求得
$$-40\leqslant t\leqslant -34.$$
取 $t=-34, -35, \cdots, -40$，相应地由 ⑭ 式求得方程 ⑬ 的全部非负整数解为 $(x, y)=(32, 1), (27, 4), (22, 7), (17, 10), (12, 13), (7, 16), (2, 19)$ 共七组．

由定理 2 不难看出，如果 $(a, b)=1$，则

(i) 当 a, b 异号时，方程 ② 一定有无穷多组非负整数解，这只要在公式 ⑩ 中取 t 为绝对值充分大的正(负)整数即可．

(ii) 当 a, b 同号时，方程 ② 至多有有限组非负整数解．

因此，我们最感兴趣的是(正系数)方程

$$ax+by=n \quad ⑮$$

的非负整数解．这里 a, b, n 都是正整数，且 $(a, b)=1$．读者或许能够料想到当 n 适当大时，方程 ⑮ 有非负整数解．事实的确如此，下面的例子给出了很精确的结果．

例 **10** 设 a, b, n 都是正整数，$(a, b)=1$，则当 $n>ab-a-b$ 时，方程

$$ax+by=n \quad ⑮$$

有非负整数解 (x, y)．$n=ab-a-b$ 时，方程没有非负整数解 (x, y)．

证明 先证明第一个结论．因 $(a, b)=1$，所以必有整数 x, y 使

$$ax+by=n.$$

我们总可以选择 x 是非负的，并且小于 b. 因为如果 x 不是这样，只需将 x 加上或减去若干个 b，并相应地将 y 减去或加上同样多的 a，便得到满足所述要求的解。

当 $n>ab-a-b$ 时，我们有

$$by=n-ax>ab-a-b-ax\geqslant ab-a-b-a(b-1)$$
$$=-b.$$

从而 $y>-1$ 也是非负整数。

当 $n=ab-a-b$ 时，方程⑮没有非负整数解。假如不然，设 (x, y) 是一组非负整数解，则有

$$ab=(x+1)a+(y+1)b,$$

所以 $a\mid(y+1)b$. 因 $(a, b)=1$，故 $a\mid y+1$，注意 $y+1>0$. 所以

$$y+1\geqslant a.$$

同理
$$x+1\geqslant b,$$

于是
$$ab=(x+1)a+(y+1)b\geqslant ab+ab=2ab,$$

这不可能．证毕．

例 10 的结论可以换一个说法：当 $(a, b)=1$, a, $b>0$ 时，$ab-a-b$ 是不能表示成 $ax+by$ $(x, y\geqslant 0)$ 形式的最大整数．一个自然的问题是：在 $0\leqslant n\leqslant ab-a-b$ 内有多少个整数 n 不能表示成上述形式？我们有如下结果．

例 11 设 $(a, b)=1$, a, $b>0$，则在 $0\leqslant n\leqslant ab-a-b$ 中，恰有 $\frac{(a-1)(b-1)}{2}$ 个整数 n 不能表示成 $ax+by$ 的形式，这里 x, y 都是非负整数．

证明　闭区间 $[0, ab-a-b]$ 中共有 $ab-a-b+1=(a-1)(b-1)$ 个整数，能写成 $ax+by$ $(x, y\geqslant 0)$ 形式的称为可表示的，否则称为不可表示的．只需证明可表示的与不可表示

的整数能两两配对，即 n 与 $A-n$（这里 $A=ab-a-b$，$0\leqslant n\leqslant A$）这两个数中恰有一个是可表示的（如果这点得到证明，则可表示的与不可表示的整数各占总数的一半，个数都等于 $\frac{(a-1)(b-1)}{2}$）。

首先，n 与 $A-n$ 不能都是可表示的．否则的话，$A=n+(A-n)$ 也是可表示的，与例 10 的结论相违背．

其次，如果 n 是不可表示的，我们证明 $A-n$ 一定是可表示的．

因为 n 是不可表示的，适合

$$n=ax+by$$

的整数 x、y（其存在性由定理 1 保证）中必有一个是负的，不妨设 $x<0$．我们还可以设 $y<a$，不然的话，将 y 减去若干个 a，并相应地将 x 加上同样多的 b，直至 y 满足 $0\leqslant y<a$（由于 n 是不可表示的，这时仍有 $x<0$）．于是

$$\begin{aligned}A-n&=ab-a-b-ax-by\\&=a(-x-1)+b(a-1-y),\end{aligned}$$

显然 $-x-1\geqslant 0$，$a-1-y\geqslant 0$，即 $A-n$ 可表示，证毕．

上面我们已经建立了二元一次不定方程的完整理论，现在转向一般的 k 元一次不定方程（$k\geqslant 3$）：

$$a_1x_1+a_2x_2+\cdots+a_kx_k=c. \qquad ⑯$$

其中 $a_i(i=1, 2, \cdots, k)$，c 都是给定的整数，$a_1a_2\cdots a_k\neq 0$．

与定理 1 类似，我们有

定理 3 方程 ⑯ 有整数解的充分必要条件是

$$(a_1, a_2, \cdots, a_k)\mid c.$$

证明可以仿照定理 1 的证法进行，我们将它留给读者.

k 元一次不定方程 ⑯ 如果有整数解，则必有无穷多组整数解，它的通解公式中含有 $k-1$ 个自由参数．这是与定理 2 平行的结论（在那里仅有一个自由参数 t）．我们不作详细讨论，而将重点放在最有实用价值的三元一次不定方程的解法上.

例 12 求不定方程

$$x+2y+3z=18 \tag{17}$$

的全部整数解.

解 将原方程写成

$$x=18-2y-3z,$$

易见其全部整数解是

$$x=18-2u-3v,\quad y=u,\quad z=v,$$

其中 u, v 是任意整数.

就题论题地求解一个具体的三元一次不定方程，其办法很多，但大体总可遵循这样一个原则，即通过像前面所述的欧氏算法那类思想，从原来的方程导出一个新的方程，与原方程相比，这个方程未知数系数的绝对值中最小者严格减少，这样进行若干次，便得到一个方程，它有一个未知数的系数为 1，即化为 ⑰ 那样的简单情形．说明这一切的最好办法莫过于举例了，请看下面的例题.

例 13 求不定方程

$$6x+20y-15z=23 \tag{18}$$

的全部整数解.

解 方程中未知数系数的绝对值以 6 为最小，我们用 6 除方程 ⑱ 的两边，得

$$x=\frac{-20y+15z+23}{6}$$

$$=-3y+2z+4+\frac{-2y+3z-1}{6},$$

于是应有整数 u，使得

$$-2y+3z-1=6u. \qquad ⑲$$

方程 ⑲ 中，未知数系数的绝对值最小者为 $2(<6)$，将 ⑲ 两边同除以 2，得到

$$y=z+\frac{z-1}{2}-3u,$$

于是应有整数 v，使得

$$z-1=2v,$$

从而 $z=2v+1$，代入 ⑲ 式得

$$y=z+v-3u=3v-3u+1,$$

于是 $\quad x=-3y+2z+4+u=10u-5v+3.$

所以方程 ⑱ 的全部整数解为

$$x=10u-5v+3,\ y=-3u+3v+1,\ z=2v+1,$$

其中 u, v 是任意整数.

例 14 求不定方程

$$25x+13y+7z=4 \qquad ⑳$$

的全部整数解.

解 方程中未知数系数的绝对值最小者是 7，用 7 除方程 ⑳ 的两端，得到

$$z=-3x-y+\frac{-4x-6y+4}{7},$$

于是有整数 t，使得

$$-4x-6y+4=7t. \qquad ㉑$$

㉑ 中未知数系数的绝对值最小者是 $4(<7)$，用 4 除 ㉑ 的两

端，得到

$$x=-y-t+1+\frac{-2y-3t}{4},$$

于是有整数 u，使得

$$-2y-3t=4u. \tag{㉓}$$

再以 $2(<4)$ 除 ㉓ 的两端，得

$$y=-2u-t-\frac{t}{2},$$

应有整数 v，使

$$t=2v,$$

以此代入方程 ㉓，有

$$y=-2u-3v,$$

从而

$$x=-y-t+1+u=3u+v+1,$$

$$z=-3x-y+t=-7u+2v-3.$$

所以方程 ㉑ 的全部整数解是

$$x=3u+v+1,\ y=-2u-3v,\ z=-7u+2v-3,$$

其中 u，v 是任意整数.

关于三元一次不定方程的非负整数解，类似于二元的情形，最令人感兴趣的也是系数全为正整数的情形. 在实际求解时，原则和以前一样，即先求出全部整数解，然后确定通解中的参数以得出非负解.

确定非负整数解的个数也是一个有趣的问题. 限于篇幅，我们仅举一个例子.

例 **15** 求出不定方程

$$x+2y+3z=18$$

的非负整数解的解数.

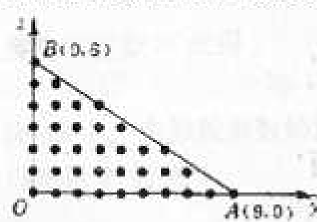
解. 由方程得到

$$2y+3z=18-x\leqslant 18,$$

作一个关于 y, z 的直角坐标系, 在该坐标系中画出线段

$$AB: 2y+3z=18 \ (y\geqslant 0,\ z\geqslant 0).$$

则问题中方程的非负整数解的数目就是三角形 OAB 内以及



边界上的整点数(整点即两个坐标都是整数的点). 不难计数得出这些点总共有37个, 即所求的解数有37组.

下面的例子类似于例10.

例16 设 a, b, c 都是正整数, $(a, b, c)=1$, 又设 $(a, b)=d$, 则当 $n>\frac{ab}{d}+cd-a-b-c$ 时, 方程

$$ax+by+cz=n \qquad ㉓$$

有非负整数解 (x, y, z).

证明 由于 $(a, b, c)=1$, 所以 $(c, d)=1$, 方程

$$cz+dt=n \qquad ㉔$$

有整数解. 我们可以选择 ㉔ 的解使得(参看例10的证明):

$$0\leqslant z<d.$$

这样, 当 $n>\frac{ab}{d}+cd-a-b-c$ 时,

$$t=\frac{n-cz}{d}\geqslant\frac{n-c(d-1)}{d}>\frac{ab}{d^2}-\frac{a}{d}-\frac{b}{d}.$$

设 $a=da_1$, $b=db_1$, 则 $(a_1, b_1)=1$, $t>a_1b_1-a_1-b_1$. 因而由例10可知, 方程

$$a_1x+b_1y=t \qquad ㉕$$

必有非负整数解 (x, y).

由方程 ㉔、㉕ 消去 t 即得 ㉓, 所以适合 ㉔ 与 ㉕ 的 x, y, z, t 一定适合 ㉓. 因此, 方程 ㉓ 有非负整数解 (x, y, z). 证毕.

从本例可推出，存在一个仅与 a, b, c 有关的正整数 $f(a, b, c)$，使得凡大于 $f(a, b, c)$ 的正整数 n，方程㉓一定有非负整数解；而当 $n=f(a, b, c)$ 时，㉓没有非负整数解．并且我们有

$$f(a, b, c) \leqslant \frac{ab}{d}+cd-a-b-c.$$

求出 $f(a, b, c)$ 是一个迄今尚未完全解决的问题．但对于某些特殊情况，我们能够做到这点．例 17 是这方面的一个结果，它曾被选作国际中学生数学竞赛的试题．

例 17 设 a, b, c 为三个正整数，满足 $(a, b)=(b, c)=(c, a)=1$，证明

$$2abc-bc-ac-ab$$

是不能表示成 $xbc+yac+zab$ 形式的最大整数．这里 x, y, z 都是非负整数．

证明 这里要证明两点：第一，证明当 $n>2abc-bc-ac-ab$ 时，

$$xbc+yac+zab=n \qquad ㉖$$

一定有非负整数解 (x, y, z)．第二，证明当 $n=2abc-bc-ac-ab$ 时，方程㉖没有非负整数解．

第一点的证明可由上例推出，只要分别用 bc, ac, ab 代替上例的 a, b, c 即可．请注意，因 a, b, c 两两互素，所以 $(bc, ac, ab)=1$．

第二点的证明与例 10 的解法相仿，用反证法．假设有非负整数 x, y, z，使得

$$xbc+yac+zab=2abc-bc-ac-ab,$$

则有

$$bc(x+1)+ac(y+1)+ab(z+1)=2abc. \qquad ㉗$$

由于 a 整除 ㉗ 的右端，故也整除它的左端，所以有

$$a \mid bc(x+1)$$

因 $(a, b)=(a, c)=1$，从而 $a \nmid bc$，这样必有

$$a \mid (x+1).$$

因 $x+1 \geqslant 1$，故 $x+1 \geqslant a$. 同理

$$y+1 \geqslant b,\ z+1 \geqslant c.$$

这就推出 ㉗ 的左端 $\geqslant 3abc$，矛盾. 证毕.

本例的结论，用我们前面的记号表示就是：如果正整数 a, b, c 两两互素，则

$$f(ab, bc, ac)=2abc-ab-bc-ac.$$

当 $a_1, a_2, \cdots, a_k$ 都是正整数，且 $(a_1, a_2, \cdots, a_k)=1$ 时，不难用数学归纳法证明，存在一个只与 $a_1, a_2, \cdots, a_k$ 有关的正整数 $f(a_1, a_2, \cdots, a_k)$，使得当 $n>f(a_1, a_2, \cdots, a_k)$ 时 $(k \geqslant 2)$，不定方程

$$a_1x_1+a_2x_2+\cdots+a_kx_k=n \tag{㉘}$$

有非负整数解 $(x_1, x_2, \cdots, x_k)$，而当 $n=f(a_1, a_2, \cdots, a_k)$ 时，㉘ 没有非负整数解[例 10 表明 $f(a_1, a_2)=a_1a_2-a_1-a_2$]. 对于 $k \geqslant 3$，具体地求出 $f(a_1, a_2, \cdots, a_k)$ 的表达式是非常困难的，这个问题称为弗罗宾纽斯 (Frobenius) 问题. 对于这类问题，著名数学家爱多斯(Erdös)告诫人们："别去碰它！" 或许我们还是忘掉它好.

二、一次不定方程组

解方程组的主要方法是消元．请先看下面的例子，一般的求解原则已体现在其中．

例 1 求出方程组

$$\begin{cases} x+y+z=100, & ① \\ 5x+3y+\dfrac{z}{3}=100 & ② \end{cases}$$

的全部整数解(x, y, z)．

解 由②，z 必须是 3 的倍数，作代换 $z=3t$，方程组化为

$$\begin{cases} x+y+3t=100, & ③ \\ 5x+3y+t=100. & ④ \end{cases}$$

我们消去 t（消去 x 或 y 当然也可以），这可以通过 3×④－③，得到

$$7x+4y=100,$$

它的通解是

$$x=-100+4u,\ y=200-7u. \qquad ⑤$$

这里 u 是任意整数．将⑤代入③或④来确定 t（代入④式较为方便），得出

$$t=u.$$

于是原方程组的全部整数解是

$$x=-100+4u,\ y=200-7u,\ z=3u,$$

其中 u 为任意整数．

例1和我国古代的一个问题有关，它就是南北朝时期的《张丘建算经》中的"百鸡问题"：

例2 公鸡5元钱1只，母鸡3元钱1只，小鸡1元钱3只．现在用100元钱去买100只鸡，问公鸡、母鸡、小鸡各应买多少只？

解 设公鸡，母鸡，小鸡的只数分别为x，y，z，依题意，得

$$\begin{cases}x+y+z=100,\\5x+3y+\frac{z}{3}=100.\end{cases}$$

这就是例1中的不定方程，现在的问题需要求出它的全部非负整数解．这等价于选择参数u，使得(见例1的通解)

$$x=-100+4u\geqslant0,\ y=200-7u\geqslant0,\ z=3u\geqslant0.$$

(与第一节例9类似)．

解上面的不等式组，得

$$25\leqslant u\leqslant\frac{200}{7},$$

因为u是整数，所以取$u=25, 26, 27, 28$，相应的$(x, y, z)=(0, 25, 75)$，$(4, 18, 78)$，$(8, 11, 81)$，$(12, 4, 84)$都是问题的答案．

例3 小城用5元钱买40个水果招待五位朋友．水果有苹果、梨子和杏子三种，每个的价格分别为20分、8分、3分．小城希望他和五位朋友都能分到苹果，并且各人得到的苹果数目互不相同，试问他能否实现自己的愿望．

解 设苹果，梨子，杏子分别买了x，y，z个，则

$$\begin{cases}20x+8y+3z=500, & ⑥\\x+y+z=40. & ⑦\end{cases}$$

⑥$-8\times$⑦，得

$$12x-5z=180.$$

它的通解是

$$x=90-5t,\ z=180-12t, \tag{8}$$

其中 t 是任意整数，将 ⑧ 代入方程 ⑦，得

$$y=-230+17t,$$

所以方程组的全部整数解是

$$x=90-5t,\ y=-230+17t,\ z=180-12t.$$

要确定正整数解，只要求出使不等式组

$$90-5t>0,\ -230+17t>0,\ 180-12t>0$$

成立的整数 t. 易解得

$$13\frac{9}{17}<t<15,$$

因此必须 $t=14$，相应的正整数解只有一组为 $(x, y, z)=(20, 8, 12)$.

不难看出，小域的愿望不能实现．因为按照他的要求，苹果至少要有

$$1+2+3+4+5+6=21>20(\text{个}).$$

上面的方程组也可以用尝试法来解．为此，先作一点观察与估计，由 ⑥ 可见 z 是 4 的倍数．由 ⑦，$z<40$，再由 ⑥ 得出

$$\begin{aligned}500&=20x+8y+3z\\&<20(x+y)+120,\end{aligned}$$

从而

$$x+y>19.$$

$$z=40-(x+y)<40-19=21,$$

这样可分别取 $z=4, 8, 12, 16, 20$ 代入方程组 ⑥，⑦ 来求相应的 x，y.

下面谈谈一般的三元一次方程组

$$\begin{cases}a_1x+b_1y+c_1z=d_1, & ⑨\\ a_2x+b_2y+c_2z=d_2 & ⑩\end{cases}$$

其中 a_1, a_2, b_1, b_2, c_1, c_2, d_1, d_2 都是整数，并且未知数的系数不全为 0.

如果 d_1, d_2 不全为 0，方程组称为非齐次的，否则称为齐次的.

齐次方程组

$$\begin{cases}a_1x+b_1y+c_1z=0, & ⑪\\ a_2x+b_2y+c_2z=0 & ⑫\end{cases}$$

一定有整数解，$(x_0, y_0, z_0)=(0, 0, 0)$ 就是一组整数解. 不仅如此，我们将要证明它有无穷多组整数解.

如果 ⑪、⑫ 左边未知数的系数成比例，那么方程组相当于一个三元一次不定方程. 由上一节，我们知道它有无穷多组整数解(习题 3 给出了通解).

如果 ⑪、⑫ 左边未知数的系数不成比例，即整数

$$A=b_1c_2-c_1b_2,\ B=c_1a_2-a_1c_2,\ C=a_1b_2-a_2b_1 \qquad ⑬$$

不全为 0. 我们称这个方程组为非退化的. 下面的例 4 给出了它的通解.

例 4 非退化的齐次不定方程组 ⑪、⑫ 有无穷多组整数解，其通解为

$$x=\frac{A}{D}t,\ y=\frac{B}{D}t,\ z=\frac{C}{D}t, \qquad ⑭$$

其中 t 是任意整数，A, B, C 由 ⑬ 给出，$D=(A, B, C)$.

证明 设 x, y, z 是方程组的一组整数解. ⑪$\times c_2-$⑫$\times c_1$，得到

$$(a_1c_2-a_2c_1)x+(b_1c_2-b_2c_1)y=0,$$

即
$$Bx=Ay.$$

同样得出 $Cx=Az,\ Cz=By.$
于是有

$$\frac{x}{A}=\frac{y}{B}=\frac{z}{C}=u. \qquad ⑮$$

这里 u 是比值(我们约定在比式中，若分母为 0，则分子也为 0).

由于 $(A,\ B,\ C)=D$，根据第一节定理 3(取 $k=3$)，存在整数 $l,\ m,\ n$，使

$$lA+mB+nC=D.$$

从而 $$u=\frac{lx+my+nz}{lA+mB+nC}=\frac{1}{D}(lx+my+nz).$$

令 $t=Du=lx+my+nz$，则 t 为整数，并且由 ⑮ 得

$$x=\frac{A}{D}t,\ y=\frac{B}{D}t,\ z=\frac{C}{D}t.$$

这就证明了方程组的任意一组整数解都具有 ⑭ 的形式．反过来，不难验证由 ⑭ 确定的 $(x,\ y,\ z)$ 是方程组的整数解．证毕．

非齐次不定方程组 ⑨、⑩ 未必有整数解．但如果有一组整数解(特解)，则必有无穷多组解．这些解与相应的齐次方程组 ⑪、⑫ 有密切的关系．实际上，非齐次方程组的通解就是它的任一个特解加上齐次方程组的通解．请看下面的例题．

例 5 设 $(x_0,\ y_0,\ z_0)$ 是非齐次不定方程组 ⑨，⑩ 的一组特解，则其通解为

$$x=x_0+\frac{A}{D}t,\ y=y_0+\frac{B}{D}t,\ z=z_0+\frac{C}{D}t, \qquad ⑯$$

其中 t 为任意整数，$A,\ B,\ C$ 由 ⑬ 式给出，$D=(A,\ B,\ C)$.

证明 不难验证，由 ⑯ 确定的三数组 $(x,\ y,\ z)$ 适合 ⑨

及 ⑯. 下面证明方程组的任意一组解(x, y, z)都具有 ⑯ 的形式. 我们有

$$\begin{cases}a_1x_0+b_1y_0+c_1z_0=d_1,\\a_2x_0+b_2y_0+c_2z_0=d_2,\end{cases}$$

与 ⑨, ⑩ 对应地相减, 得到

$$\begin{cases}a_1(x-x_0)+b_1(y-y_0)+c_1(z-z_0)=0,\\a_2(x-x_0)+b_2(y-y_0)+c_2(z-z_0)=0.\end{cases}$$

这就化成了齐次的方程, 由例 4 的结论知道存在整数 t, 使

$$x-x_0=\frac{A}{D}t,\ y-y_0=\frac{B}{D}t,\ z-z_0=\frac{C}{D}t.$$

即 ⑯ 成立. 证毕.

应用通解结构的理论(例 5)来解三元不定方程组, 主要有两步:

第一, 求出通解 ⑯ 中自由参数 t 的系数 $\frac{A}{D}, \frac{B}{D}, \frac{C}{D}$ (我国古代称之为增减数).

第二, 求出一个特解. 这可以采用尝试法: 先假定一个未知数, 例如 z, 为某一确定的整数值(常常用 0), 然后解出其他两个未知数. 如果都是整数, 那么就得到一组特解. 否则, 再令 z 为其他整数值, 继续尝试.

请读者回顾一下前面的例题.

当然, 也会遇到无整数解的情况, 下面的两个例题就是这样.

例 6 判断方程组

$$\begin{cases}3x+10y-z=11,\\8x-13y+2z=1\end{cases} \qquad ⑰$$

是否有整数解.

解 消元法仍然是有效的手段．将第一个方程乘2然后加上第二个方程，得到

$$14x-7y=23.$$

这个方程显然没有整数解，所以方程组⑰也无解．

判断方程组无整数解并不是非消元不可．下面例7的解法就是很机灵的．

例7 证明方程组

$$\begin{cases}2x+4y-7z=1,\\-7x+6y-18z=23\end{cases} \tag{18}$$

没有整数解．

证明 假设⑱有一组整数解(x, y, z)，将两个方程相加，

$$-5x+10y-25z=24,$$

即
$$5(-x+2y-5z)=24.$$

上式左边被5整除，但右边不能，矛盾，所以无整数解．

现在我们考虑另一种类型的问题：

例8 一堆棋子，三三数之余2，五五数之余3，七七数之余4．求这堆棋子的个数．

解 设棋子有n个，则

$$\begin{cases}n=3x+2,\\n=5y+3,\\n=7z+4,\end{cases} \tag{19}$$

这里x、y、z都是非负整数．

消去n得到x、y、z的三元方程组

$$\begin{cases}3x-5y=1, & (20)\\5y-7z=1, & (21)\end{cases}$$

为得到这个方程组的特解，先取$y=1$来尝试，由⑳得$x=2$，

但 z 却不是整数. 将 y 换为 4, 7, 10. 相应的 x 总是整数. 最后得出整数解 $x=17$, $y=10$, $z=7$. 不难算出增减数为 35, 21, 15. 所以 $x=17+35t$ (y、z 不必写出),

$$n=3x+2=53+105t,\ t\in Z. \qquad ㉒$$

于是, 棋子的个数为 $53+105t$, t 为非负整数. 最少个数是 53(取 $t=0$).

例 9 求出整数 n, 它的 2 倍被 3 除余 1, 3 倍被 5 除余 2, 5 倍被 7 除余 3.

解 由题意可知,

$$\begin{cases} 2n=3x+1, & ㉓ \\ 3n=5y+2, & ㉔ \\ 5n=7z+3. & ㉕ \end{cases}$$

$3\times$㉓$-2\times$㉔, 得(我们故意采用与上例不全相同的解法)

$$9x-20y=1,$$

易于求出其通解为

$$x=-1-20u,\ y=-1-9u,$$

其中 u 为任意整数. 代入 ㉓, 得

$$n=-1-15u. \qquad ㉖$$

将 ㉖ 代入 ㉕, 便有

$$7z+75u=-8,$$

其通解是 $\qquad z=-44+75t,\ u=4-7t.$

从而 $\qquad n=-61+105t,\ t\in Z.$

这种类型的问题, 我国古代称为"韩信点兵". 它也可以用同余的理论来处理, 请参看华罗庚先生的《从孙子的神奇妙算谈起》, 本书不予讨论.

某些特殊问题, 可以用较简捷的方法得出答案.

例 10 求大于 1 的最小正整数 n, 使它被 2, 3, 5, 7, 9

除得的余数都是1.

解　$n-1$是2, 3, 5, 7, 9的倍数，所以n的最小值是$2\times5\times7\times9+1=631$.

例11　求最小的正整数n，使$\frac{n}{2}$是一个整数的平方，$\frac{n}{3}$是一个整数的立方，$\frac{n}{5}$是一个整数的五次方.

解　可以设n没有2, 3, 5以外的素因子，即n的形式为

$$n=2^a\times3^b\times5^c,$$

这里a, b, c都是正整数. 要求出最小的正整数a, b, c，使得

$a-1, b, c$都是2的倍数，

$a, b-1, c$都是3的倍数，

$a, b, c-1$都是5的倍数.

由于a是3和5的倍数，所以a是15的倍数. 设$a=15k$(k为正整数)，在k为奇数时，$15k-1$被2整除，从而k的最小正值为1，即a的最小值为15. 同样b, c的最小值分别为2×5与2×3. 于是n的最小值为$2^{15}\times3^{10}\times5^6$.

对于更多个变数的一次方程组，我们关心的是(具有某种性质的)解的存在性. 下面的国际数学竞赛题就是一例.

例12　方程组

$$\begin{cases}a_{11}x_1+a_{12}x_2+\cdots+a_{1q}x_q=0,\\a_{21}x_1+a_{22}x_2+\cdots+a_{2q}x_q=0,\\\cdots\cdots\\a_{p1}x_1+a_{p2}x_2+\cdots+a_{pq}x_q=0\end{cases}$$

中，$q=2p$, $a_{ij}\in\{-1, 0, +1\}$ $(1\leqslant i\leqslant p,\ 1\leqslant j\leqslant q)$. 证明这个方程组必有满足下列条件的整数解$(x_1, x_2, \cdots, x_q)$：

(i) $x_1, x_2, \cdots, x_q$不全为0.

(ii) 对所有的 $j(1\leqslant j\leqslant q)$, $|x_j|\leqslant q$.

证明 我们采用抽屉原理来证明.

设 $b_i=a_{i1}y_1+a_{i2}y_2+\cdots+a_{iq}y_q \quad (i=1, 2, \cdots, p)$, 其中 y_j 为整数, $0\leqslant y_j\leqslant q$, $j=1, 2, \cdots, q$.

每个 y_j 有 $q+1$ 种取法, 因而 $(y_1, y_2, \cdots, y_q)$ 有 $(q+1)^q$ 种, 两两不同. 相应的 $(b_1, b_2, \cdots, b_p)$ 也就有 $(q+1)^q$ 个.

另一方面, 设 r_i 是 $a_{i1}, a_{i2}, \cdots, a_{iq}$ 中 $+1$ 的个数, 则其中 -1 的个数不超过 $q-r_i$. 因此

$$(r_i-q)q\leqslant b_i\leqslant r_iq.$$

这样, b_i 至多能取 $r_iq-(r_i-q)q+1=q^2+1$ 个不同的值. p 元数组 $(b_1, b_2, \cdots, b_p)$ 至多有 $(q^2+1)^p$ 种.

由于 $q=2p$, 所以

$$(q+1)^q=(q+1)^{2p}=(q^2+2q+1)^p>(q^2+1)^p.$$

根据抽屉原理, 必有两个不同的 $(y_1, y_2, \cdots, y_q)$ 产生的 $(b_1, b_2, \cdots, b_p)$ 是相同的. 设 $(y'_1, y'_2, \cdots, y'_q)\neq(y''_1, y''_2, \cdots, y''_q)$ 产生出同样的 $(b_1, b_2, \cdots, b_p)$. 令

$$x_j=y'_j-y''_j, \quad (j=1, 2, \cdots, q)$$

则 $x_1, x_2, \cdots, x_q$ 不全为 0, 并且对所有的 $j(1\leqslant j\leqslant q)$,

$$|x_j|=|y'_j-y''_j|\leqslant q.$$

由于对所有的 $i(1\leqslant i\leqslant p)$,

$$\begin{aligned}&a_{i1}x_1+a_{i2}x_2+\cdots+a_{iq}x_q\\&=a_{i1}(y'_1-y''_1)+a_{i2}(y'_2-y''_2)+\cdots+a_{iq}(y'_q-y''_q)\\&=(a_{i1}y'_1+a_{i2}y'_2+\cdots+a_{iq}y'_q)-(a_{i1}y''_1+a_{i2}y''_2+\cdots+a_{iq}y''_q)\\&=b_i-b_i=0,\end{aligned}$$

$x_1, x_2, \cdots, x_q$ 就是满足要求的解.

例 13 设 $1\leqslant m<n$, $a_{ij}(1\leqslant i\leqslant m, 1\leqslant j\leqslant n)$ 都是整数, 则不定方程组

$$\begin{cases} a_{11}x_1+a_{12}x_2+\cdots+a_{1n}x_n=0, \\ a_{21}x_1+a_{22}x_2+\cdots+a_{2n}x_n=0, \\ \cdots\cdots \\ a_{m1}x_1+a_{m2}x_2+\cdots+a_{mn}x_n=0 \end{cases} \quad ㉗$$

有一组不全为 0 的整数解 $(x_1, x_2, \cdots, x_n)$，满足

$$|x_j| \leqslant (A_1A_2\cdots A_m)^{\frac{1}{n-m}} \quad (1 \leqslant j \leqslant n),$$

这里 $A_i=|a_{i1}|+|a_{i2}|+\cdots+|a_{in}|>0 \quad (1 \leqslant i \leqslant m)$。

证明 与例 12 类似，令

$$b_i=a_{i1}y_1+a_{i2}y_2+\cdots+a_{in}y_n \quad (1 \leqslant i \leqslant m),$$

其中 y_j 为整数，满足 $0 \leqslant y_j \leqslant N(1 \leqslant j \leqslant n)$，而 N 是待定整数.

设 B_i 为 $a_{i1}, a_{i2}, \cdots, a_{in}$ 中正数的和，则其中负数的和为 B_i-A_i. 从而 $(B_i-A_i)N \leqslant b_i \leqslant B_iN$，$b_i$ 至多有 A_iN+1 种不同的整数值. 只要 N 满足

$$(N+1)^n>(A_1N+1)(A_2N+1)\cdots(A_mN+1), \quad ㉘$$

则方程组 ㉗ 就有不全为 0 的解 $(x_1, x_2, \cdots, x_m)$ 满足 $|x_j| \leqslant N(1 \leqslant j \leqslant m)$.

取 $N=[(A_1A_2\cdots A_m)^{\frac{1}{n-m}}]$，这里 $[x]$ 表示 x 的整数部分，则

$$\begin{aligned}(N+1)^n &= (N+1)^m \cdot (N+1)^{n-m} \\ &> (N+1)^m(A_1A_2\cdots A_m) \\ &= (NA_1+A_1)(NA_2+A_2)\cdots(NA_m+A_m) \\ &\geqslant (NA_1+1)(NA_2+1)\cdots(NA_m+1).\end{aligned}$$

因此，㉗ 有合乎要求的解.

注 1：例 12 是本例的特殊情况.

注 2：待定的整数 N，只需满足不等式 ㉘，因而有较大的选择余地. 对于某些具体的方程组，有可能导出更好的（$|x_j|$ 的界更小）结果.

三、分　　解

有些不定方程，我们称之为可分解的方程，能够用分解的方法来处理．这里所说的分解包含着整数与整式的分解．

整数的唯一分解定理，平方差、立方和差等乘法公式都是常用的工具．

例 1　求不定方程

$$x^2-y^2=105$$

的全部正整数解 (x, y)．

解　利用平方差公式得

$$(x+y)(x-y)=3\times5\times7.$$

由唯一分解定理，便得到如下几种可能的情况（注意 $x+y$ 是正的，从而 $x-y$ 也是正的并且小于 $x+y$）：

$$\begin{cases}x-y=1,\\x+y=3\times5\times7;\end{cases}\quad\begin{cases}x-y=3,\\x+y=5\times7;\end{cases}$$

$$\begin{cases}x-y=5,\\x+y=3\times7;\end{cases}\quad\begin{cases}x-y=7,\\x+y=3\times5,\end{cases}$$

解这四个方程组，得 $(x, y)=(53, 52), (19, 16), (13, 8), (11, 4)$．

例 2　证明方程

$$x^3+11^3=y^3$$

没有正整数解 (x, y)．

证明　假设方程有解，显然 $0<x<y$．将方程移项并分

解，得

$$(y-x)(y^2+xy+x^2)=11^3.$$

由原方程得出 $y^3>11^3$，即 $y>11$，所以

$$y^2+xy+x^2>11^2.$$

利用唯一分解定理可知(本题开始时为什么先移项，又为什么要估计 y^2+xy+x^2 的大小，到这一步就很清楚了)：

$$y-x=1,\ y^2+xy+x^2=11^3.$$

消去 y，得 $$(x+1)^2+x(x+1)+x^2=11^3,$$

即 $$3(x^2+x)=1330.$$

但 $3\nmid 1330$，矛盾。

注：例 2 是所谓的费尔马 (Fermat) 大定理（本书第九节）的特殊情形。

下面举一个有无限多组解的不定方程。

例 3　求不定方程

$$2x^2+5xy-3xz-5y+3z=5$$

的全部正整数解 (x, y, z)。

解　将方程左边看作 x、y 的二次式，用所谓双十字相乘法知道再减去 2 便可以分解，即原方程可变为

$$(x-1)(2x+5y-3z+2)=3.$$

由唯一分解定理（注意 $x>0$）：

$$\begin{cases}x-1=1,\\2x+5y-3z+2=3;\end{cases} \quad ①$$

或

$$\begin{cases}x-1=3,\\2x+5y-3z+2=1.\end{cases} \quad ②$$

先解方程组 ①，显然 $x=2$，所以

$$3z-5y=3,$$

其通解为

$$y=3+3t,\ z=6+5t,\ t \text{ 为任意整数}.$$

这样，① 的全部正整数解是

$$x=2,\ y=3+3t,\ z=6+5t,\ t \text{ 为非负整数}. \quad ③$$

同样可求得方程组 ② 的全部正整数解是

$$x=4,\ y=3+3t,\ z=8+5t,\ t \text{ 为非负整数}. \quad ④$$

原方程的全部正整数解由 ③、④ 给出.

可分解方程不同于一次方程(组)，它没有完整的理论与固定的解法可循，我们难以断定一个方程能否分解．即使能够分解，有时不知怎样分解，有时因为分解方式较多而难以选择．这里有很多初等的技巧，解法因题而异．唯一可以奉献给读者的忠告是：尝试，尝试，再尝试．如果一条道路毫无成功的希望，就应当另辟新的途径．

判明一个乘积中的各个因式互素往往是非常重要的，例 4，例 5 均是如此．

例 4 证明：没有正整数 x, y，满足

$$x(x+1)=y^2. \quad ⑤$$

证明 设 ⑤ 式成立．因为正整数 x 和 $x+1$ 互素，它们的积为完全平方，由唯一分解定理推出 x, $x+1$ 都是完全平方．设

$$x+1=u^2,\ x=v^2,\ uv=y,\ u>v.$$

则
$$u^2-v^2=1,$$

即
$$(u-v)(u+v)=1.$$

这只有
$$u-v=1,\ u+v=1,$$

解得 $u=1$, $v=0$，从而 $x=0$．矛盾．

注 1：本题可以用第四节例 7 的方法来解．

注 2："两个正整数的平方差不能为 1"，这一点用简单的估计也不难得出，请参见第四节例 4.

例 5 证明：连续三个正整数之积不能是一个正整数的 k 次方幂．这里 k 是给定的正整数，且 $k\geqslant 2$．

证明 假设有正整数 $x\geqslant 2$ 及 y 使

$$(x-1)x(x+1)=y^k.$$

请注意上面左端的三个因式 $x-1$, x, $x+1$ 并非两两互素，因此不能推出它们都是 k 次方幂．克服这个困难的一种办法是将方程变形为

$$(x^2-1)x=y^k,$$

这时，因为 x 和 x^2-1 是互素的，所以有正整数 u, v 使得

$$x=u^k,\ x^2-1=v^k,\ uv=y,\ v>1.$$

我们有 $1=u^{2k}-v^k=(u^2)^k-v^k$

$$=(u^2-v)(u^{2k-2}+u^{2k-4}v+\cdots+u^2v^{k-2}+v^{k-1}).$$

由于 $x\geqslant 2$，从而 $u\geqslant 2$，又已知 $k\geqslant 2$，故 $u^{2k-2}+u^{2k-4}v+\cdots+v^{k-1}>1$．导出矛盾．

分解后，有时需要讨论奇偶性（即与第五节的同余方法结合使用）．

例 6 求不定方程

$$x^4+y^4+z^4=2x^2y^2+2y^2z^2+2x^2z^2+24$$

的全部整数解．

解 关键的一步（也是第一个困难）是看出方程可分解成（这与求三角形面积的海仑——秦九韶公式密切相关）

$$(x+y+z)(x+y-z)(y+z-x)(z+x-y)=-2^3\times 3. \quad ⑥$$

由于 ⑥ 式右端被 2 整除，故 2 一定也整除左端，即左边四个因式中至少有一个是偶数．另一方面，这四个因式同奇同偶，故都是偶数，即 ⑥ 的左端被 2^4 整除，但 $2^4\nmid 2^3\times 3$，因此方程无整数解．

上面的论证，用同余的语言来说，就是先对 ⑥ 模 2，然后

对 ⑥ 模 16. 这一方法在第五节中还要详细讨论.

在“指数方程”中，常常根据指数的奇偶性，分为几种情况处理.

例 7　设整数 x, y 都大于 1，求方程

$$x^y=2^z-1$$

的全部正整数解 (x, y, z).

解　显然 x^y 是奇数，从而 x 也是，将方程写成

$$x^y+1=2^z. \tag{7}$$

这时有两种情况：当 y 是奇数时，上式可分解为

$$(x+1)(x^{y-1}-x^{y-2}+\cdots-x+1)=2^z. \tag{8}$$

⑧ 式左端第二个因式是奇数(y) 个奇数的和，故是奇数. 但它是 2^z 的因数，所以只能是 1. 于是 ⑧ 成为

$$x+1=2^z,$$

从而 $y=1$, 与题设矛盾. 这就证明了当 y 为奇数时，方程无解.

当 y 为偶数时，设

$$y=2k,\ k\geqslant 1,\ x^k=2l+1.$$

这样　$x^y+1=(x^k)^2+1=(2l+1)^2+1=4l(l+1)+2$.

它能被 2 整除，但不能被 4 整除，由 ⑦，z 必须为 1 (否则，若 $z\geqslant 2$, 则 ⑦ 的右边被 4 整除). 这就推出 $x=1$, 与题设相违，故此时方程也无解.

例 8　求出方程

$$x^y=2^z+1$$

的全部正整数解，其中 $y>1$.

解　求解方法和上例中所用过的方法相似，分为两种情况：

当 y 是奇数时，将方程分解成

$$(x-1)(x^{y-1}+x^{y-2}+\cdots+x+1)=2^z.$$

因为 x 是奇数，$y>1$，所以 $x^{y-1}+x^{y-2}+\cdots+x+1>1$ 是奇数，与上例一样，此时方程无解．

当 y 是偶数时，设 $y=2k$，$k\geqslant 1$．因 x^k 是奇数，设它为 $2l+1\,(l\geqslant 1)$，则原方程化为

$$(x^k)^2-1=2^z,$$

即
$$4l(l+1)=2^z. \qquad ⑨$$

如果 $l>1$，则 l，$l+1$ 这两个连续整数中必有一个是大于1的奇数，故有奇素数 p 整除 $l(l+1)$，但 p 不能整除 ⑨ 的右端，所以，$l>1$ 时方程无解．而当 $l=1$ 时，$x=3$，$y=2$，及 $z=3$，于是所求的解为 $(x, y, z)=(3, 2, 3)$．

注：例7及本例都是著名的卡塔兰(Catalan)猜想的特殊情况．

卡塔兰猜想　除了 $8=2^3$，$9=3^2$ 之外，没有两个连续的正整数都是完全方幂，即不定方程

$$x^m-y^n=1,\ m>1,\ n>1.$$

仅有一组正整数解

$$x=3,\ y=2,\ m=2,\ n=3.$$

这一有趣的猜想十分难证，经过许多数学家的努力，现在已基本解决(参见下节末)．

有些不定方程组也能用分解的方法处理．这时，经常需要用消元法．

例9　求出所有边长为整数，且面积(的数值)等于周长的直角三角形．

解　设这直角三角形三边之长分别为正整数 x, y, z，$x\leqslant y<z$．依题意，得方程组

$$\begin{cases}x^2+y^2=z^2,\\ x+y+z=\dfrac{1}{2}xy.\end{cases}$$

消去 z, 我们有

$$x^2+y^2=\left(\frac{1}{2}xy-x-y\right)^2,$$

即
$$(x-4)(y-4)=8.$$

于是
$$(x-4)\mid 8,\ (y-4)\mid 8.$$

当 $x<4$ 时, 只能有 $x=2$ 或 $x=3$, 相应的 y 为 0 或 -4, 均不可能, 从而 $x-4>0$. 又 $x-4\leqslant y-4$, 这样 $x-4$ 只能为 1 或 2. 求得 $x=5$ 或 6, 相应的 y 为 12 或 8, 于是全部解是 $(x, y, z)=(5, 12, 13), (6, 8, 10)$.

例 10 求不定方程组

$$\begin{cases}x+y+z=3,\\ x^3+y^3+z^3=3\end{cases}$$

的全部整数解.

解 从方程组消去 z, 得到

$$8-9x-9y+3x^2+6xy+3y^2-x^2y-xy^2=0,$$

变形为

$$8-3x(3-x)-3y(3-x)+xy(3-x)+y^2(3-x)=0,$$

即
$$(3-x)(3x+3y-xy-y^2)=8.$$

由此得出 $(3-x)\mid 8$, 从而

$$3-x=\pm1,\ \pm2,\ \pm4,\ \pm8,$$

即 $x=-5, -1, 1, 2, 4, 5, 7, 11$ (如果有解, 则必在其中!), 逐一代入原方程检验, 不难得出全部整数解是 $(x, y, z)=(1, 1, 1), (-5, 4, 4), (4, -5, 4), (4, 4, -5)$.

通过分解确定解的取值范围 ($a\mid b$ 就意味着 $|a|\leqslant|b|$), 然后逐一验证, 这也是常用方法之一.

我们已经看到了分解的作用, 应当指出, 这一方法是建立在唯一分解定理这一基础上的. 唯一分解定理是代数数论的

中心内容之一，借此机会我们简单地作一点介绍.

代数数论研究的对象是代数数域. 数域是一个非空数集，其中的元素作加、减、乘、除（除数非0）后所得结果仍在这个集中. 例如全体有理数是一个数域，记为 Q. 全体实数、复数也都是数域[⑩]. 如果域中每个数都是一个整数系数代数方程的根，这个域便称为代数数域. 例如 Q 是代数数域. 把 $i=\sqrt{-1}$ 与有理数进行加减乘除得到的数域

$$Q(i)=\{\alpha+\beta i \mid \alpha,\ \beta\in Q\}$$

也是代数数域. 显然 $Q(i)$ 包含 Q. 全体整数 Z 称为 Q 的整数环. 它的特点是，非0、非单位（即 ± 1）的整数都能唯一地分解成素数的积. $Q(i)$ 中也可以定义"整数环"，它就是

$$Z(i)=\{a+bi \mid a,\ b\in Z\},$$

称为高斯(Gauss)整数环. $Z(i)$ 中任意两个数的加、减、乘都在其中. 与 Z 相似，能够在 $Z(i)$ 中定义"整除"，"单位"，"素数"等概念. 不过，两者也有差别，例如数5在 Z 中是素数，但在 $Z(i)$ 中则不是. $Z(i)$ 中也能建立唯一分解定理，即非0及非单位的"整数" $a+bi(a,\ b\in Z)$ 可以"唯一地"分解成 $Z(i)$ 中"素数"和"单位"的积. 有了这个定理，许多不定方程可以放到 $Z(i)$ 中来考虑.

研究发现，有些代数数域的"整数环"上有唯一分解定理，而有些则不然. 对于不具有唯一分解性质的"整数环"，也有人想出了补救的办法，这就是加入"理想数". 代数数论是在对不定方程（尤其是第九节中的费尔马大定理）研究的推动下形成起来的，反过来又为处理不定方程提供了有力的工具. 这是现代数学中最有活力的领域之一.

四、估　计

我们已经知道，不定方程未必有整数解．要判定它何时有解往往是很困难的事．然而却有一个简单的准则，有时能帮助我们证明它无整数解．这只要注意，方程如有整数解，则它当然就有实数解．换句话说，如无实数解，则它不会有整数解．这便是方程有整数解的一个必要条件．以此为出发点，有时能够有效地处理问题．先看一个简单的例子．

例1　证明方程

$$x^2+y^2+1=2xy$$

没有整数解．

证明　将方程配方成为

$$(x-y)^2+1=0,$$

它显然没有实数解，所以更不会有整数解．

也可以用代数不等式来证（实质是一样的）：方程左边

$$x^2+y^2+1\geqslant 2xy+1>2xy,$$

从而它无解．

这里处理问题的角度和上节处理的很不相同，虽然一般情况下并非像例1那样简单，但论证的原则是类似的．对于某些方程，我们将它放在一个更大的范围——实数域中来考虑，有时能够估计出方程的实数解的（有限）范围．因一个有限范围内的整数至多有有限个，过渡到整数（我们关心的是方程的整数解），就能够对可能的情况逐一检验，以确定方程

解的情况，不仅判明了方程有、无解，也能求出（如果仅有有限组的话）全部解．这就是估计方法的大意，其实质就是估计方程整数解（的绝对值）的上界．

例2　求方程

$$x^2+xy+y^2=49$$

的全部正整数解 (x, y)．

解　不妨设 $x\leqslant y$，从原方程得出

$$3x^2\leqslant x^2+xy+y^2=49,$$

即

$$x\leqslant\sqrt{\frac{49}{3}}.$$

上面这个界限是对实数 x 而言的，过渡到正整数，则得 $x\leqslant4$，即 x 只可能取 1, 2, 3, 4, 分别代入原方程检验，不难求得方程的正整数解为 $(x, y)=(3, 5)$．由对称性，还有一组解是 $(x, y)=(5, 3)$．

本题也可以换一个解法．

将原方程看作是关于 y 的一元二次方程，它有实数解的充分必要条件是

$$x^2-4(x^2-49)\geqslant0,$$

即

$$x\leqslant2\sqrt{\frac{49}{3}}.$$

这里得到的 x 的上界比前面的大，虽然也能解决问题，但检验的次数增加了．

例3　求方程

$$x+y=x^2-xy+y^2$$

的全部整数解．

解　将方程看作 x 的一元二次方程，变形为

$$x^2-(y+1)x+y^2-y=0.$$

我们先寻求它有实数解的条件，得

$$(y+1)^2-4(y^2-y)\geqslant 0,$$

即 $$1-\frac{2\sqrt{3}}{3}\leqslant y\leqslant 1+\frac{2\sqrt{3}}{3}.$$

在上述范围内，整数 y 只可能是 0, 1, 2. 逐一代入原方程，可求出其全部整数解是 $(x, y)=(0, 0), (1, 0), (0, 1), (2, 1), (1, 2), (2, 2)$ 共六组.

例 2、例 3 中的方程都是椭圆的方程，其实数解是有界的.

有一些方程的实数解是无界的，从而上面那种证明就不能奏效. 但仍可用估计的方法来处理. 这时，我们应着眼于整数，应用整数的特性来估计.

例 4 证明两个正整数的平方差不能是 1.

证明 用反证法. 假设有正整数 x, y，使

$$x^2-y^2=1. \qquad ①$$

请注意方程 ① 的实数解有无穷多并且是无界的. 我们着眼于整数. 由 ① 显然有 $x>y$，因为 x, y 都是整数，所以

$$x\geqslant y+1$$

（这是一种简单、但常常用到的技巧），从而

$$x^2-y^2\geqslant(y+1)^2-y^2=2y+1\geqslant 2\times 1+1=3,$$

和 ① 矛盾.

例 5 证明不存在四个互不相同的正整数 x, y, z, t，使得 $x^x+y^y=z^z+t^t$.

证明 本题的唯一困难就在于它看上去似乎很难.

不妨设四个不同的正整数中，x 最大. 则有

$$x-1\geqslant t,\ x-1\geqslant z,$$

从而 $$x^x+y^y>x^x=x\cdot x^{x-1}\geqslant x^{x-1}+x^{x-1}\geqslant x^t+x^z>t^t+z^z.$$

所以方程 $x^4+y^4=t^4+z^4$ 无互不相同的正整数解.

例 6 证明不存在正整数 x, y, 使得 x^2+y 及 $x+y^2$ 都是完全平方.

证明 假设有正整数 x, y 及 u, v, 使得

$$x^2+y=u^2, \tag{②}$$

$$x+y^2=v^2. \tag{③}$$

从 ② 式易见 $u>x$, 即 $u\geqslant x+1$, 所以

$$y=u^2-x^2\geqslant(x+1)^2-x^2=2x+1>x,$$

同样从 ③ 式可知, $x>y$. 矛盾.

通过 ②、③ 消元是一种"走火入魔"的做法.

在两个连续正整数的 k 次幂之间没有正整数的 k 次幂. 这一简单的性质也是不定方程中常常用到的.

例 7 证明不定方程

$$x(x+1)+1=y^2$$

没有正整数解.

证明 对 $x>0$, 我们有代数不等式

$$x^2<x(x+1)+1<(x+1)^2.$$

因此, 当 x 为正整数时, $x(x+1)+1$ 界于两个相邻的完全平方数之间, 从而它不会是平方数. 证毕.

本题也能用分解的方法来证明. 请读者自己完成.

例 8 证明不存在四个连续正整数, 其积是整数的完全立方.

证明 假设有整数 $x\geqslant2$ 及 y, 使

$$(x-1)x(x+1)(x+2)=y^3. \tag{④}$$

当 x 为奇数时, $(x, x+2)=(x, 2)=1$. 此外, 由于相邻整数互素, 所以 x 与 $x-1$, $x+1$ 都互素. 从而 x 与 $(x-1)(x+1)(x+2)$ 互素. 由 ④ 可知, 存在整数 u, v, 使得

$$(x-1)(x+1)(x+2)=u^3,\ x=v^3.$$

另一方面，$(x-1)(x+1)(x+2)=x^3+2x^2-x-2$ 满足不等式（注意 $x\geqslant 2$）：

$$x^3<x^3+2x^2-x-2<(x+1)^3,$$

即界于两个相邻整数的三次方幂之间，故它不能是三次方幂 u^3，矛盾。

当 x 为偶数时，同理可证明，$x+1$ 与 $(x-1)x(x+2)$ 互素，由 ④ 推出它们都是三次方幂。但 $(x-1)x(x+2)=x^3+x^2-2x$，满足（除非 $x=2$）

$$x^3<x^3+x^2-2x<(x+1)^3,$$

因此，当 $x\neq 2$ 时，$(x-1)x(x+2)$ 不是三次方幂，矛盾。当 $x=2$ 时，④式左边为 24，也不是完全立方。证毕。

例 9 证明连续四个正整数的积不能是整数的 k 次方幂，这里 $k\geqslant 2$ 是给定的整数。

证明 $k=2$ 的情形见习题 15. $k=3$ 时，见上例。下面考虑 $k\geqslant 4$。假设有整数 $x\geqslant 2$ 及 y，使

$$(x-1)x(x+1)(x+2)=y^k.$$

(i) 当 x 为奇数时，x 和 $(x-1)(x+1)(x+2)$ 互素（参见上例的论证），从而有整数 u, v, 使得

$$x=u^k,\ (x-1)(x+1)(x+2)=v^k. \qquad ⑤$$

我们只需证明，当 $x\geqslant 2$, $k\geqslant 3$ 时，$(x-1)(x+1)(x+2)=x^3+2x^2-x-2$ 界于两个相邻数的 k 次方幂之间，从而它本身不能是 k 次方幂。事实上，

$$\begin{aligned}(u^3)^k=x^3&<x^3+2x^2-x-2<x^3+kx^2+1\\&=u^{3k}+k\cdot u^{2k}+1<u^{3k}+k\cdot u^{3(k-1)}+1\\&<(u^3+1)^k.\end{aligned}$$

(ii) 当 x 为偶数时，$x+1$ 与 $(x-1)x(x+2)$ 互素，所以它

们都是 k 次方幂．设整数 u, v 使

$$x+1=u^k,\ (x-1)x(x+2)=v^k. \qquad ⑥$$

一方面，易知

$$(x-1)x(x+2)<(x-1)(x+1)^2<(x+1)^3=(u^3)^k;$$

另一方面，

$$\begin{aligned}(x-1)x(x+2)&=(u^k-2)(u^k-1)(u^k+1)\\&=u^{3k}-2u^{2k}-u^k+2>u^{3k}-ku^{2k}\\&=((u^3-1)+1)^k-ku^{2k}\\&>(u^3-1)^k+k(u^3-1)^{k-1}-ku^{2k}\\&>(u^3-1)^k.\end{aligned}$$

[最后一步是由于 $(u^3-1)^{k-1}=(u-1)^{k-1}(u^2+u+1)^{k-1}>(u-1)^3u^{2(k-1)}>u^{2k}$．]

这样，$(x-1)x(x+2)$就不能为 k 次方幂．证毕．

更一般地，爱多斯证明了：

任意 $n(\geqslant 2)$ 个连续正整数的积不可能是整数的 k 次方幂．这里 $k\geqslant 2$．

由此立即推出，在 $n>1$ 时，$n!$ 不是 $k(>1)$次方幂．请见习题 16．

例 10　求方程

$$x^2+x=y+y^2+y^3+y^4 \qquad ⑦$$

的全部整数解．

解　先将 ⑦ 的两边同乘 4（这一"招"简单实用），使左端成为平方，得

$$(2x+1)^2=4(y^4+y^3+y^2+y)+1,$$

从而在 $y\neq -1$ 时

$$(2x+1)^2>4y^4+4y^3+y^2=(2y^2+y)^2. \qquad ⑧$$

另一方面，只要

$$y^2>2y, \quad ⑨$$

就有

$$(2x+1)^2<4y^4+4y^3+y^2+2(2y^2+y)+1$$
$$=(2y^2+y+1)^2,$$

即$(2x+1)^2$在两个相邻的平方数之间，这(与例7相同)是不可能的．因此，$y=-1$或⑨不成立．于是整数y必须满足：$-1\leqslant y\leqslant 2$，即$y=-1, 0, 1, 2$．由此不难求得方程的全部解是$(x, y)=(0, 0), (-1, 0), (0, -1), (-1, -1), (-6, 2), (5, 2)$．

有些方程，直接观察或稍作变形就能看出它至多只能有有限组解．这时，作较为精细的估计为解题提供了一种"求解"的途径．

例 11 求不定方程

$$xy+yz+zx=xyz+2 \quad ⑩$$

的全部正整数解．

解 因为方程右端的积(三次式)一般应大于左边的和(二次式)，有希望用估计来求解．由对称性，不妨设$x\leqslant y\leqslant z$．将方程化为

$$\frac{1}{x}+\frac{1}{y}+\frac{1}{z}=\frac{2}{xyz}+1, \quad ⑪$$

则
$$1<\frac{2}{xyz}+1=\frac{1}{x}+\frac{1}{y}+\frac{1}{z}\leqslant\frac{3}{x},$$

即$x\leqslant 2$．

当$x=1$时，由⑪得

$$y+z=2,$$

易见$y=z=1$．

当$x=2$时，由⑪有

$$\frac{1}{y}+\frac{1}{z}=\frac{1}{yz}+\frac{1}{2},$$

从而 $$\frac{2}{y}>\frac{1}{y}+\frac{1}{z}=\frac{1}{yz}+\frac{1}{2}>\frac{1}{2},$$

即 $$\frac{1}{y}>\frac{1}{4},$$

推出 $y\leqslant 3$. 我们又有

$$\frac{1}{y}+\frac{1}{yz}<\frac{1}{y}+\frac{1}{z}=\frac{1}{yz}+\frac{1}{2},$$

即 $$\frac{1}{y}<\frac{1}{2}.$$

从而 $y\geqslant 3$. 这样必有 $y=3$, 于是 $z=4$. 这样原方程的全部正整数解是 $(x, y, z)=(1, 1, 1), (2, 3, 4), (2, 4, 3), (3, 2, 4), (3, 4, 2), (4, 3, 2), (4, 2, 3)$.

例 12 设 a, b 是正整数, a^2+b^2 被 $a+b$ 除得的商是 q, 余数为 r, 求出所有的使 $q^2+r=1977$ 的有序数对 (a, b).

解 由题设, $a^2+b^2=q(a+b)+r\ (0\leqslant r<a+b)$. 由最简单的估计得

$$\begin{aligned}\frac{(a+b)^2}{2}\leqslant a^2+b^2&=q(a+b)+r\\&<(a+b)(q+1)\\&\leqslant(\sqrt{1977}+1)(a+b),\end{aligned}$$

可见, 数对 (a, b) 至多有有限个. 要确定所有的 (a, b), 需要较为精细的估计.

我们有 $$\begin{aligned}r<a+b\leqslant\frac{2(a^2+b^2)}{a+b}&=2q+\frac{2r}{a+b}\\&<2q+2,\end{aligned}$$

即 $$r\leqslant 2q+1.$$

于是 $$(q+1)^2=q^2+2q+1\geqslant q^2+r=1977\geqslant q^2,$$

从而 $q=[\sqrt{1977}]=44$, $r=1977-q^2=41$.

$$a^2+b^2=44(a+b)+41,$$

配方成为 $$(a-22)^2+(b-22)^2=1009.$$
不妨设$(a-22)^2\geqslant(b-22)^2$，则
$$1009\geqslant(a-22)^2\geqslant 500,$$
$$31\geqslant|a-22|\geqslant 23.$$
这样通过检验不难得到 $|a-22|=28$，$|b-22|=15$. 即 $a=50$，$b=7$ 或 $a=50$，$b=37$. 所求的有序数对是 $(a, b)=(50, 7)$，$(50, 37)$，$(7, 50)$，$(37, 50)$.

有些不定方程初看起来，不能立即断定它至多只有有限组解.如果我们相信(或者说猜测)事实上如此的话，估计方法实际上提供了一种"尝试"的手段. 请注意，哪怕只改变方程的一个常数，问题的难度和解的情况就可能有很悬殊的差别，这正是不定方程的困难与复杂之处. 例如，简单的估计可证明方程
$$x(x+1)=y^2$$
没有正整数解. 但是，方程
$$x(x+1)=2y^2$$
却有无穷多组正整数解(见第七节例 2). 对于有无穷多组解的方程，费力去估计解的界限，其结果注定是不幸的.

下面的例子都采用估计的方法. 但如何进行估计，则不尽相同. 正如下棋一样，重要的不是生搬硬套，而是根据问题的特点，灵活处理.

例 **13** 求出不定方程
$$x^3+x^2y+xy^2+y^3=8(x^2+xy+y^2+1)$$
的全部整数解.

解 将方程分解成为
$$(x^2+y^2)(x+y-8)=8(xy+1) \quad ⑫$$
我们作如下的估计.

假设 $x+y-8\geqslant 6$, 则 $x+y\geqslant 14$, 从而

$$x^2+y^2\geqslant \frac{(x+y)^2}{2}>4,$$

这时 ⑫ 的左端

$$\begin{aligned}&\geqslant 6(x^2+y^2)=4(x^2+y^2)+2(x^2+y^2)\\&\geqslant 8xy+2(x^2+y^2)>8(xy+1),\end{aligned}$$

故此时方程无整数解.

当 $x+y-8\leqslant -4$ 时, $x+y\leqslant 4$, 则 ⑫ 的左端

$$\leqslant -4(x^2+y^2)\leqslant -4\times 2|xy|<8xy+1,$$

此时方程亦无整数解. 因此, 方程的整数解 (x, y) 应满足

$$-3\leqslant x+y-8\leqslant 5.$$

另一方面, ⑫ 的左端应是偶数, 这推出 x, y 的奇偶性必须相同, 从而 $x+y-8$ 是偶数, 所以它只可能是 -2, 0, 2, 4. 再结合 ⑫, 通过检验不难得知, 所求的整数解为 $(x, y)=(2, 8)$, $(8, 2)$.

例 14 设 p 是两个相邻正整数之积, $p>6$. 证明方程

$$\sum_{i=1}^{p} x_i^2-\frac{4}{4p+1}\left(\sum_{i=1}^{p} x_i\right)^2=1 \qquad ⑬$$

没有整数解 x_1, x_2, $\cdots$, x_p.

证明 设 $p=k(k+1)$, $k\geqslant 3$, 则

$$p\geqslant 12. \qquad ⑭$$

设方程 ⑬ 有整数解 $x_1\geqslant x_2\geqslant\cdots\geqslant x_p$. 用恒等式

$$\left(\sum_{i=1}^{p} x_i\right)^2=p\left(\sum_{i=1}^{p} x_i^2\right)-\sum_{1\leqslant i<j\leqslant p}(x_i-x_j)^2,$$

可将 ⑬ 化为

$$\sum_{i=1}^{p} x_i^2+4\sum_{1\leqslant i<j\leqslant p}(x_i-x_j)^2=4p+1. \qquad ⑮$$

如果所有的 x_i $(i=1, 2, \cdots, p)$ 都相等, 那么由 ⑮ 得

$$4p+1=px_1^2,$$

右边被 p 整除，但左边不被 p 整除，这不可能.

于是，必有整数 l 使得

$$x_1\geqslant x_2\geqslant\cdots\geqslant x_l>x_{l+1}\geqslant\cdots\geqslant x_p.$$

当 $p-1>l\geqslant 2$ 时，由于 $x_1, x_2, \cdots, x_l$ 中每一个与 $x_{l+1}, \cdots, x_p$ 中每一个的差的平方至少为 1,

$$4\sum_{1\leqslant i<j\leqslant p}(x_i-x_j)^2\geqslant 4l(p-l)\geqslant 8(p-2)>4p+1$$

这和 ⑮ 矛盾.

所以 $l=1$ 或 $p-1$. 不妨设 $l=1$, 即

$$x_1>x_2=x_3=\cdots=x_{p-1}\geqslant x_p.$$

这时 ⑮ 成为

$$\sum_{i=1}^{p}x_i^2+4((p-2)(x_1-x_2)^2+(x_1-x_p)^2+(p-2)(x_p-x_2)^2)$$
$$=4p+1,$$

从而 $x_1-x_2=1$（否则上式左端大于右端），上式即

$$4(x_1-x_p)^2+(p-2)(x_p-x_2)^2+\sum_{i=1}^{p}x_i^2=9.$$

要使上式左端不大于右端，必须 $x_p=x_2$, 从而

$$x_1^2+(p-1)x_2^2=5.$$

由于 $p\geqslant 12$, x_2 必须为 0. 但这时 $x_1=1$, 上式仍不成立. 因此方程 ⑬ 没有整数解.

例 15 确定所有的正整数 n, 使方程

$$x^3+y^3+z^3=nx^2y^2z^2 \qquad ⑯$$

有正整数解 (x, y, z).

解 $n=3$ 显然合乎要求，相应的方程有解 $x=y=z=1$. 下面我们证明必有 $n=1$ 或 3.

不妨设 $x\geqslant y\geqslant z>0$, 将方程变形为

$$n=\frac{x}{y^2z^2}+\frac{y}{x^2z^2}+\frac{z}{y^2x^2},\tag{17}$$

容易求得右端后两项的上界．要估计第一项，需确定 x（用 y, z 表示）的上界．由原方程得

$$y^3+z^3=x^2(ny^2z^2-x)\geqslant x^2.$$

这样从 ⑰ 得到

$$n\leqslant\frac{\sqrt{y^3+z^3}}{y^2z^2}+\frac{y}{y^2z^2}+\frac{z}{y^2z^2}$$

$$=\sqrt{\frac{1}{y^4z}+\frac{1}{yz^4}}+\frac{1}{yz^2}+\frac{1}{y^2z}.\tag{18}$$

很明显，当 $z\geqslant2$ 时，由于 $y\geqslant z$，从 ⑱ 推出 $n<\frac{1}{2}$．因此只有 $z=1$ 才能有正整数 n 使方程 ⑯ 有解．

当 $y\geqslant2$ 时（注意 $z=1$），由 ⑱ 可得 $n<\frac{3}{2}$，所以此时只能有 $n=1$．相应的方程有解 $(x, y, z)=(3, 2, 1)$．

当 $y=1$ 时，从 $x^2\leqslant y^3+z^3=2$，可得 $x=1$，因此必须 $n=3$，相应的方程有解 $(x, y, z)=(1, 1, 1)$．

下面的例子是美国中学生的数学竞赛题．

例 16　求出不定方程

$$(a^2+b)(a+b^2)=(a-b)^3$$

所有的非零整数解．

解　先考虑平凡情况．

当 $a=b$ 时，易得解为 $a=b=-1$．以下设 $a\neq b$．

当 a, b 中恰有一个为 0 时，不妨设 $a=0$，则易知 $b=1$．对称地还有一组解 $a=1$, $b=0$．

如果 a, b 都大于 0．由对称性，设 $a>b$，则由原方程得出

$$a^3<(a^2+b)(b^2+a)=(a-b)^3<a^3,$$

矛盾. 故此时无整数解.

如果 a, b 都小于 0, 不妨设 $0>a>b$, 则有

$$(0<)\, b^2+a \leqslant (a^2+b)(b^2+a)=(a-b)^2,$$

即
$$a \leqslant a^2-2ab,$$
推出
$$2b+1 \geqslant a,$$
矛盾. 此时仍无整数解.

现在考虑 a, b 异号的情形, 不妨设 $a>0$, $b<0$. 我们在原方程中用 $-b$ 代替 b, 得

$$(a^2-b)(b^2+a)=(a+b)^2. \qquad ⑲$$

下面来求 ⑲ 的全部正整数解.

显然 $a>1$(否则 ⑲ 的左端 $\leqslant 0$). 设 $(a, b)=d$, $a=a_1d$, $b=b_1d$, $(a_1, b_1)=1$, $d\geqslant 1$. 将 ⑲ 变形为

$$a_1[a_1b_1^2d^2+a_1(da_1-1)-3b_1]=b_1^2(db_1+1), \qquad ⑳$$

推出 b_1 整除 ⑳ 的左端. 由于 $(a_1, b_1)=1$, 故 $b_1 \mid (da_1-1)$.

因为 $da_1-1=a-1>0$, 所以由 $b_1 \mid (da_1-1)$ 导出 $b_1 \leqslant da_1-1$(这也是简单而实用的方法). 当 $da_1-1=1$ 时, $a=da_1=2$. 易知这时(19)的解是 $a=2$, $b=1$ $(d=1)$. 当 $da_1-1\geqslant 2$ 时, ⑳(从而 ⑲)无正整数解. 事实上, ⑳ 的左端减右端(注意 $da_1-1\geqslant 2$)

$$\begin{aligned}
&\geqslant (b_1+1)da_1b_1^2+a_1^2(da_1-1)-3a_1b_1-b_1^2(db_1+1)\\
&=db_1^2(a_1-1)+a_1^2(da_1-1)+b_1^2(da_1-1)-3a_1b_1\\
&\geqslant 2a_1^2+2b_1^2-3a_1b_1\geqslant 4a_1b_1-3a_1b_1>0.
\end{aligned}$$

这样便求出原方程的全部非零整数解是: $(a, b)=(0, 1)$, $(1, 0)$, $(-1, -1)$, $(-1, 2)$, $(2, -1)$.

在第一节中, 我们已经提到关于不定方程的三个问题, 即判断它是否有解, 是否有无穷组解与求出全部解. 是否有解当然是最基本的. 1900 年, 伟大的德国数学家希尔伯特(D.

Hilbert)在展望本世纪数学前景的演讲中提出23个问题，其中就有一个是关于不定方程的.

希尔伯特第十问题　设$f(x_1, x_2, \cdots, x_n)$是整系数多项式. 是否能用一种由有限步构成的一般算法来判断不定方程

$$f(x_1, x_2, \cdots, x_n)=0$$

有无整数解?

希尔伯特相信有这样的算法. 然而事实并不像这位现代数学的总设计师所期望的那样美好. 1970年, 苏联的马蒂塞维奇利用数理逻辑与罗宾逊等人的结果证明: 第十问题的答案是否定的.

既然不存在一般的算法，那么对某些特殊类型的方程，要断定它有无整数解，往往依靠估计，首先找出解的上界. 因此，对不定方程的解(的绝对值)作上界估计是现代数学研究中的一个重要课题. 在这方面有很多出色的工作，例如(在第三节例8的注中提到的)卡塔兰猜想已基本解决. 这个结果可以叙述如下:

设正整数m, n都大于1, 如果方程

$$k=x^m, \quad k+1=y^n$$

有正整数解(x, y)，则$k\leqslant 10^{10^{10^{10}}}$.

这样, 只要能对不大于$10^{10^{10^{10}}}$的正整数逐一验证就可以彻底解决问题. 然而这个上界委实太大(但它的的确确是一个有限的数!), 目前还无法办到. 在上界不是很大时，高速计算机能够助人一臂之力，求出相应方程的全部整数解.

五、同　余

同余(请参见附录)是数论中最基本的概念之一，有着非常广泛的应用．本节利用同余证明一些不定方程无解或者仅有某种性质的解．

假设 $f(x_1, x_2, \cdots, x_n)$ 是整系数多项式．如果不定方程

$$f(x_1, x_2, \cdots, x_n)=0 \quad ①$$

(至少)有一组整数解 $x_1', x_2', \cdots, x_n'$，则对于任意正整数 m，同余式

$$f(x_1, x_2, \cdots, x_n)\equiv 0 \pmod m \quad ②$$

也有整数解．这是很明显的，因为 $f(x_1', x_2', \cdots, x_n')$ 等于 0，被 m 除得的余数当然是 0．所以，$x_1=x_1', x_2=x_2', \cdots, x_n=x_n'$ 便是 ② 的一组解．这样，我们就得到方程 ① 有整数解的一个必要条件：同余式 ② 对任意正整数 m 都有整数解．换句话说，如果能找到一个正整数 m 使 ② 无解，则 ① 必然也无解．这就是用同余证明不定方程无整数解的原则．请注意，在第四节中曾经指出，方程 ① 有整数解的必要条件之一是它必须有实数解，那是将 ① 放在"较大"的范围(即实数域)中考虑．而现在，我们则着眼于"较小"的范围——模 m 的完全剩余系．下面的例子是这种想法的具体体现．

例 1　证明不定方程

$$x^2+x+1=2y^2 \quad ③$$

没有整数解．

证明　将方程改写成

$$x(x+1)+1=2y^2. \qquad ④$$

如果 ④ 有整数解，将 ④ 模 2，也就是考虑奇偶性．右边是偶数，而左边的 $x(x+1)$ 是两个连续整数之积，它一定是偶数，从而 $x(x+1)+1$ 是奇数．两边的奇偶性不同，矛盾．

例 2　证明当 n 为"半偶数"，即 $n=4k+2$ 时，方程

$$x^2-y^2=n \qquad ⑤$$

无解．

证明　由 ⑤ 得

$$(x+y)(x-y)=n, \qquad ⑥$$

因为 n 是偶数，所以 ⑥ 的左边也是偶数．由于 $x+y(=x-y+2y)$ 与 $x-y$ 的奇偶性相同，$x+y$ 与 $x-y$ 必须全为偶数．但这时 ⑥ 的左边被 4 整除，右边不被 4 整除，矛盾．

另一种证法是直接模 4．注意 $x\equiv0, 1, 2, 3 \pmod 4$ 得出 $x^2\equiv0, 1 \pmod 4$．同样 $y^2\equiv0, 1 \pmod 4$．考虑所有可能的组合，得到

$$x^2-y^2\equiv0, 1, -1 \pmod 4,$$

而 ⑤ 式右边 $\equiv2 \pmod 4$，所以 ⑤ 无解．

第二种证法中指明"偶数的平方被 4 整除，奇数的平方除以 4 余 1"．这个结论颇有用处．

除考虑奇偶性（即模 2）外，常常考虑模 3, 5, 7 等素数（它们的剩余类的个数比较少，因而比较方便）以及它们的幂 4, 8, 9, 25 等．

例 3　证明不定方程

$$x^2+y^2-8z^3=6$$

没有整数解 (x, y, z)．

证明　模 2 可知 x、y 奇偶性必须相同；模 4 可知 x、y 均

应为奇数，都不足导出矛盾．所以我们进一步模 8．先将整数按模 8 分类，即对任意整数 x，有

$$x\equiv 0,\ \pm1,\ \pm2,\ \pm3,\ 4(\bmod 8)$$

之一．将上面每个同余式都平方，得出

$$x^2\equiv 0,\ 1,\ 4,\ 1,\ 0(\bmod 8),$$

即对任意一个整数 x，

$$x^2\equiv 0,\ 1,\ 4(\bmod 8). \tag{7}$$

换句话说，x^2 被 8 除所得的余数有三种可能：0，1，4．

同样，对任意整数 y，

$$y^2\equiv 0,\ 1,\ 4(\bmod 8).$$

所以，$x^2+y^2-8z^3$ 模 8 的可能值是（穷举所有的组合）0，1，2，4，5，不能为 6，即

$$x^2+y^2-8z^3\not\equiv 6(\bmod 8).$$

或者说，原方程模 8 无解，从而它没有整数解．证毕．

解答中的同余式⑦很有用处，值得记住．

例 4　如果 $n\equiv 4(\bmod 9)$，证明不定方程

$$x^3+y^3+z^3=n \tag{8}$$

没有整数解 (x, y, z)．

证明　考虑模 9，我们先确定一个整数的三次方对于模 9 能够取哪些值．要做到这一点，可以把整数 x 按模 9 分类，对每一个类来考察（如同上例中的方法）．但实际上，将 x 模 3 分类就够了．

如果 $x\equiv 0(\bmod 3)$，则显然 $x^3\equiv 0(\bmod 9)$．

如 $x\equiv 1(\bmod 3)$，设 $x=3k+1$，则

$$x^3=9k(3k^2+3k+1)+1,$$

它模 9 为 1．当 $x\equiv -1(\bmod 3)$ 时，则有 $-x\equiv 1(\bmod 3)$，故

$$-x^3\equiv(-x)^3\equiv 1(\bmod 9),$$

即 $x^3\equiv -1 \pmod 9$，从而

$$x^3\equiv 0,\ 1,\ -1 \pmod 9.$$

同样，对任意整数 y, z 也有

$$y^3,\ z^3\equiv 0,\ 1,\ -1 \pmod 9.$$

列举所有可能的组合，可知

$$x^3+y^3+z^3\equiv 0,\ 1,\ 2,\ 3,\ 6,\ 7,\ 8 \pmod 9.$$

而已知 $n\equiv 4 \pmod 9$，所以方程⑧模 9 无解．从而⑧不会有整数解．

由本例可知，存在无穷多个整数不能表示成三个整数的立方和．一个著名的问题：是否所有的整数都能表示成四个整数的立方和，迄今仍未解决．然而我们却可证明：任何整数都是五个整数的立方和(请见第六节例 8)．

下面是一道美国中学生数学竞赛题．

例 5 确定方程

$$\sum_{i=1}^{14} x_i^4=1599$$

的全部非负整数解 $(x_1,\ x_2,\ \cdots,\ x_{14})$（不计排列次序）．

解 本题和例 4 有类似之处，差别在于，那里容易看出应当模 9（题中已经出现了 mod 9），而现在则不易意识到，模 16 就能够证明方程无整数解．

之所以选择 16，是因为方程左边已经有 14 项，剩余类的个数 $\geqslant 15$ 才比较有希望导出矛盾(我们采用同余证明方程无整数解)．而 $15=3\times 5$，（根据著名的中国剩余定理)它相当于模 3 与模 5 的作用，不能解决问题．

我们先来确定，对整数 x, x^4 模 16 能为哪些值．

不必将 x 模 16 分类，当 x 为偶数时，显然

$$x^4\equiv 0 \pmod{16};$$

当x为奇数时，由⑦，x^2具有$8k+1$的形式(k是整数)，所以

$$x^4=16k(4k+1)+1,$$

即
$$x^4\equiv 1 \pmod{16}.$$

这样，任意整数的四次方对于模16只有0，1两个可能值，从而$\sum_{i=1}^{14}x_i^4$对于模16的所有可能值是0，1，2，…，14（唯独不能取15）．但$1599=1600-1\equiv -1\equiv 15 \pmod{16}$，因此原方程无解．

上面的论证实际表明，如果$n\equiv 15 \pmod{16}$，则方程

$$\sum_{i=1}^{14}x_i^4=n$$

没有整数解．

不过数学竞赛的问题不会用这种形式提出，因为既已挑明以16为模，难度就大大降低了．

用估计方法考虑例5，似乎不够明智．因为$x_i\leqslant\sqrt[4]{1599}<7(1\leqslant i\leqslant 14)$，仍有$7^{14}$种组合供选择，要判断方程是否有解，需要作很复杂的检验．试想一下，如果方程中的常数项改成$2^{800}+15$（这时也无解！），那就更令人望而却步了．

用同余处理问题，核心在于选择适当的模．究竟怎样选择，我们无法提供放之四海而皆准的法则．实际上，不可能也不应该有任何扼杀问题"活力"的法则，对于解题者来说，虽然某些例题可供借鉴，但更重要的是依靠自己去观察问题的特点，通过尝试找到正确的途径．

例6 证明不定方程

$$2x^2-5y^2=7$$

没有整数解．

证法一 由原方程不难看出，y是奇数（实际上是对方程

模2). 模8. 注意

$$y^2\equiv1 \pmod 8),$$

我们有 $$2x^2\equiv5y^2+7\equiv5+7\equiv4 \pmod 8),$$

即 $$x^2\equiv2 \pmod 4).$$

但 $x^2\equiv1, 0 \pmod 4)$, 故上式不能成立, 从而原方程无解.

证法二 模7, 得到

$$2x^2\equiv5y^2+7\equiv5y^2\equiv-2y^2 \pmod 7),$$

即 $$2(x^2+y^2)\equiv0 \pmod 7).$$

因为 $(2, 7)=1$, 这就推出

$$x^2+y^2\equiv0 \pmod 7).$$

不难检验, 整数的平方模7只可能是0, 1, 2, 4之一, 这样, 要使上面的同余式成立, 必须有 $x\equiv y\equiv0 \pmod 7)$. 令

$$x=7x_1,\ y=7y_1,\ x_1, y_1 \text{ 都是整数},$$

代入原方程, 得到

$$7(2x_1^2-5y_1^2)=1,$$

这显然是不可能的.

有时先将方程适当变形, 以便考虑余数的可能情况.

例7 证明不定方程

$$x^2-2xy^2+5z+3=0$$

没有整数解 (x, y, z).

证明 将方程(左边配方)变形为

$$(x-y^2)^2-y^4+5z+3=0. \qquad ⑤$$

考虑模5. 不难验证, 一个整数的平方模5只能是0, ±1, 因此

$$(x-y^2)^2\equiv0, \pm1 \pmod 5),$$

$$y^4=(y^2)^2\equiv0, 1 \pmod 5).$$

所以⑤式左边模5只能是1, 2, 3, 4, 恰不为0, 故原方程无

整数解.

例 8　证明方程

$$5m^2-6mn+7n^2=1985$$

没有整数解.

证明　将原方程变形为

$$(5m-3n)^2+26n^2=5\times 1985.$$

模 13 得

$$(5m-3n)^2\equiv 5\times 1985\equiv 6 \pmod{13}, \qquad ⑩$$

但对于 $x\equiv 0, \pm 1, \pm 2, \pm 3, \pm 4, \pm 5, \pm 6 \pmod{13}$（按模 13 分类），$x^2\equiv 0, 1, 4, 9, 3, 12, 10 \pmod{13}$，从而整数的平方模 13 不能为 6，和 ⑩ 矛盾．因此原方程无整数解.

用估计方法也能得出证明，但需作些验证．将原方程看作关于 m 的一元二次方程，应有

$$(-6n)^2-4\times 5\times 7n^2+4\times 1985\geqslant 0,$$

即

$$n^2\leqslant \frac{1985}{26}<77.$$

（这一点也可从上面解答中的配方得到）从而

$$|n|\leqslant 8.$$

我们看到，本例用同余来论证，比估计要简洁得多．此外，下面的方程不是椭圆，估计似乎就不易奏效了.

例 9　证明不定方程

$$x^2+3xy-2y^2=122$$

没有整数解.

证明　将方程配方成

$$(2x+3y)^2=17y^2+4\times 122.$$

模 17 得

$$(2x+3y)^2\equiv 12 \pmod{17}. \qquad ⑪$$

另一方面，和上例一样不难验证，一个整数的平方对于模 17 只可能取 0, 1, 2, 4, 8, 9, 13, 15, 16 之一，不能为 12. 这与 ⑪ 矛盾.

同余的作用主要是导出一些有解的必要条件(条件不能满足时，方程无解)，对解或方程中的参数(尤其是幂指数)提出一些限制，以帮助论证与求解．关键当然是选择适当的模．有时需要取几次模，有时需要将同余与其他方法结合起来．总之，同余是一种非常灵活的方法，只有通过模仿与实践才能逐步掌握．下面再举一些例子供读者参考.

例 **10** 求所有的正整数 m, n, 使得

$$1!+2!+\cdots+m!=n^2. \qquad ⑫$$

解 不难验证，$(m, n)=(1, 1)$, $(3, 3)$ 都是解．当 $m=4, 5$ 时，问题无解．下面，我们用同余来证明当 $m\geqslant5$ 时，方程 ⑫ 没有正整数解.

模 5. 显然

$$1!+2!+3!+4!=33\equiv3 \pmod 5;$$

而当 $k\geqslant5$ 时，$k!\equiv0 \pmod 5$．于是，对 $m\geqslant5$, 有

$$1!+2!+\cdots+m!\equiv3 \pmod 5.$$

但 n^2 只能 $\equiv0, \pm1 \pmod 5$．因此，$m\geqslant5$ 时方程无解.

例 **11** 求全部正整数 m, n, 使得 $|12^m-5^n|=7$.

解 (i) 先考虑

$$12^m-5^n=-7. \qquad ⑬$$

将 ⑬ 模 4, 因为 $5\equiv1 \pmod 4$, 故有 $5^n\equiv1 \pmod 4$, 从而 ⑬ 的左边

$$12^m-5^n\equiv0-1\equiv-1 \pmod 4),$$

但右边 $\equiv1 \pmod 4$, 矛盾．所以 ⑬ 没有正整数解.

(ii) 再考虑

$$12^m=5^n+7.\qquad ⑭$$

⑭显然有解 $m=n=1$. 下面证明当 $m>1, n>1$ 时它无正整数解.

模 3, 因为

$$5^n+7\equiv(-1)^n+7\equiv(-1)^n+1 \pmod 3),$$

由⑭得, $\qquad (-1)^n+1\equiv0 \pmod 3$,

于是 n 为奇数. 设 $n=2k+1(k>0)$, 由于奇数 5^k 的平方模 8 为 1,

$$5^n=5\cdot(5^k)^2\equiv5\times1\equiv5 \pmod 8).$$

对⑭模 8, 就有($m\geqslant2$, 故 $8|12^m$)

$$0\equiv5^n-1\equiv5-1\equiv4 \pmod 8).$$

矛盾. 这样, 所求的正整数解只有一组, 即 $m=n=1$.

例 12 求出所有的正整数 m, n, 使 2^m+3^n 是完全平方.

解 考虑不定方程

$$2^m+3^n=x^2.\qquad ⑮$$

显然, x 为奇数, 且 $3\nmid x$, 从而 $x^2\equiv1 \pmod 3$. ⑮模 3 得

$$1\equiv2^m\equiv(-1)^m \pmod 3),$$

因此 m 是偶数. 设 $m=2k(k\geqslant1)$, 由于 x 为奇数, $m\geqslant2$, ⑮模 4 得出

$$1\equiv3^n\equiv(-1)^n \pmod 4),$$

从而 n 是偶数. 设 $n=2l$, 将⑮变形为

$$(x+3^l)(x-3^l)=2^{2k},\qquad ⑯$$

由⑯可知, $x+3^l$ 及 $x-3^l$ 都是 2 的方幂, 但两者的和 $2x$ 不是 4 的倍数, 从而

$$x-3^l=2,\ x+3^l=2^{2k-1}.$$

由以上两式消去 x 得

$$3^l+1=2^{2k-2}. \quad ⑰$$

如果 $k=2$, 则 $l=1$, 于是 $m=4$, $n=2$. 如果 $k>2$, 将 ⑰ 模 8, 右边 $\equiv 0 \pmod 8$, 而 $3^l\equiv 1$ 或 $3 \pmod 8$, 所以 ⑰ 的左边 $\equiv 2$ 或 $4 \pmod 8$. 这时 ⑰ 无解. 从而所求的全部解是 $(m, n)=(4, 2)$.

下面是两道国际数学竞赛题.

例 13 也是卡塔兰猜测的特殊情况(参见第三节例 8).

例 13 证明不定方程

$$x^n+1=y^{n+1}$$

没有正整数解 (x, y, n), 其中 $(x, n+1)=1$, $n>1$.

证明 显然 $y>1$. 原方程可分解成

$$(y-1)(y^n+y^{n-1}+\cdots+y+1)=x^n. \quad ⑱$$

关键是证明, $y-1$ 与 $y^n+y^{n-1}+\cdots+y+1$ 互素. 即 $y-1$ 的每一个素因数都不整除 $y^n+y^{n-1}+\cdots+y+1$.

设素数 $p\mid y-1$, 则由 ⑱, $p\mid x$. 根据已知 $(x, n+1)=1$ 得 $p\nmid(n+1)$. 另一方面,

$$y\equiv 1 \pmod p,$$

故对 $0\leqslant i\leqslant n$, 有

$$y^i\equiv 1 \pmod p.$$

将这 $n+1$ 个同余式相加, 得到

$$y^n+y^{n-1}+\cdots+y+1\equiv n+1 \pmod p.$$

因此, 由 $p\nmid(n+1)$ 得 $p\nmid(y^n+y^{n-1}+\cdots+y+1)$.

由于 p 是 $y-1$ 的任一个素因数, 所以

$$(y-1, y^n+\cdots+y+1)=1.$$

这样, 由 ⑱ 推出, 存在整数 a, b, 使得

$$y-1=a^n,\ y^n+\cdots+y+1=b^n,\ ab=x.$$

但是

$$y^n<y^n+y^{n-1}+\cdots+1<(y+1)^n,$$

从而 $y^n+\cdots+y+1$ 不能是整数的 n 次幂. 这和已得结果矛盾. 证毕.

不定方程组也可用同余来处理.

例 14 设正整数 d 不等于 2, 5, 13. 证明集合 $\{2, 5, 13, d\}$ 中可找到两个不同数 a, b, 使 $ab-1$ 不是平方数.

证明 用反证法. 设有整数 x, y, z, 使得

$$2d-1=x^2, \tag{19}$$

$$5d-1=y^2, \tag{20}$$

$$13d-1=z^2. \tag{21}$$

由 ⑲ 可知, x 是奇数, 从而

$$x^2\equiv1(\bmod 4).$$

对 ⑲ 模 4 得

$$2d-1\equiv1(\bmod 4),$$

即

$$2d\equiv2(\bmod 4),$$

$$d\equiv1(\bmod 2), \tag{22}$$

d 为奇数, 所以由 ⑳、㉑ 可知 y、z 都是偶数. 设 $y=2y_1$, $z=2z_1$. ㉑ 减去 ⑳ 得 $y^2-z^2=8d$, 即

$$y_1^2-z_1^2=2d. \tag{23}$$

但由 ㉒ 及例 2, ㉓ 不可能成立.

有些整式方程, 常数项为 0, 这种方程必有整数解: 未知数均为 0 就是它的解, 通常称为平凡解. 其他的整数解(如果有的话)称为非平凡解.

采用同余可以证明一些方程仅有平凡解.

例 15 证明不定方程

$$x^2-3y^2=2z^2 \tag{24}$$

仅有平凡解.

证明 假设 ㉔ 有非平凡解 x, y, z. 如果 $(x, y, z)=d>1$，令 $x=dx_1$, $y=dy_1$, $z=dz_1$，代入 ㉔ 后两边约去 d^2，得

$$x_1^2-3y_1^2=2z_1^2,$$

这时，$(x_1, y_1, z_1)=1$.

因此，不妨假设 ㉔ 中，$(x, y, z)=1$（凡齐次方程均可以这样做）.

模 3. 因为整数的平方模 3 为 0 或 1，所以 ㉔ 的左边 $\equiv 0, 1 \pmod 3$，右边 $\equiv 0, 2 \pmod 3$. 要两边相等必须 $x\equiv z\equiv 0 \pmod 3$. 设

$$x=3x_1, \ z=3z_1$$

代入 ㉔ 并化简得 $3x_1^2-y^2=3z_1^2$. 从而 $3\mid y^2$. 但 3 是素数，所以 $3\mid y$, $(x, y, z)\geqslant 3$. 这与所设的 $(x, y, z)=1$ 矛盾. 从而 ㉔ 只有平凡解.

例 16 证明存在无穷多个正整数 a，使不定方程

$$x^2+y^2=az^2 \qquad ㉕$$

仅有平凡解.

证明 在例 2 中，我们已经知道 $x^2\equiv 0, 1 \pmod 4$. 因此 $x^2+y^2\equiv 0, 1, 2 \pmod 4$，唯缺一个剩余类 3. 看来（猜测）$a\equiv 3 \pmod 4$ 可能使 ㉕ 仅有平凡解（如果模 3，x^2+y^2 可跑遍 3 的剩余类，所以我们模 4 而不模 3）. 下面证明确实如此.

与上例相同，可设 $(x, y, z)=1$. 如果 z 为奇数，则上面已经说过 ㉕ 的左边 $\not\equiv 3 \pmod 4$. 如果 z 为偶数，则由 ㉕ 得

$$x^2+y^2\equiv 0 \pmod 4,$$

从而 x、y 都必须是偶数，$2\mid(x, y, z)$ 与所设 $(x, y, z)=1$ 矛盾.

因此，在 $a\equiv 3 \pmod 4$ 时，㉕ 仅有平凡解. 这样的 a 当然有无穷多个.

例 17　设 k 为偶数，证明

$$x^2+y^2+z^2=kxyz \tag{㉖}$$

仅有平凡解.

证法一　设㉖有非平凡解．如果 $(x, y, z)=d>1$，那么令 $x=x_1d$, $y=y_1d$, $z=z_1d$，代入㉖并化简得

$$x_1^2+y_1^2+z_1^2=kd\cdot x_1y_1z_1. \tag{㉗}$$

㉗仍是一个㉖形的方程，只不过用偶数 kd 代替了偶数 k，$(x_1, y_1, z_1)=1$．所以，我们不妨设 $(x, y, z)=1$.

考虑奇偶性可知 x、y、z 中至少有一个是偶数．这时，㉖的右边被 4 整除．与上例相同，推出左边的另两个数也都是偶数．矛盾.

证法二　设㉖有非平凡解．由于 k 为偶数，考虑奇偶性可知 x、y、z 中至少有一个是偶数．再模 4（与证法一相同）即知 x、y、z 均为偶数．设 $x=2x_1$, $y=2y_1$, $z=2z_1$，则由㉖得

$$x_1^2+y_1^2+z_1^2=2kx_1y_1z_1. \tag{㉘}$$

对㉘进行同样的推理，可知 x_1、y_1、z_1 均为偶数，设 $x_1=2x_2$, $y_1=2x_2$, $z_1=2z_2$，代入㉘得

$$x_2^2+y_2^2+z_2^2=4kx_2y_2z_2. \tag{㉙}$$

x_2、y_2、z_2 又必须都是偶数．如此继续下去，我们推出，x、y、z 能被 2 的任意次幂整除．而这只有当 $x=y=z=0$ 时才有可能.

以上两种证法实质上是一致的（例 15，16 也是如此）．这种手法就是在第九节中要详加讨论的无穷递降法.

我们再看一个类似的例子.

例 18　设 k, l 都是非负整数．证明

$$x^2+y^2+z^2=4^k(8l+7) \tag{㉚}$$

没有整数解.

证明 先设 $k=0$. 由例3, $x^2\equiv 0, 1, 4 \pmod 8$. 所以

$$x^2+y^2+z^2\equiv 0, 1, 2, 3, 4, 5, 6 \pmod 8.$$

唯独缺7这类. 因此方程㉚无整数解.

如果 $k>0$, 由㉚得

$$x^2+y^2+z^2\equiv 0 \pmod 4.$$

与上例相同, 这时必须有

$$x\equiv y\equiv z\equiv 0 \pmod 2.$$

设 $x=2x_1$, $y=2y_1$, $z=2z_1$ (x_1, y_1, z_1 是整数),

代入㉚, 得

$$x_1^2+y_1^2+z_1^2=4^{k-1}(8l+7). \quad ㉛$$

如果 $k-1>0$, 再模4, 从㉛又推出 x_1, y_1, z_1 都是偶数. 设

$$x_1=2x_2,\ y_1=2y_2,\ z=2z_2\ (x_2,\ y_2,\ z_2 \text{ 是整数}),$$

代入㉛得

$$x_2^2+y_2^2+z_2^2=4^{k-2}(8l+7).$$

如果 $k-2>0$, 对上式继续模4, 如此等等, 反复这样做下去, 我们最终可将方程㉚中4的幂指数化为0, 而得到

$$x_k^2+y_k^2+z_k^2=8l+7, \quad ㉜$$

其中 x_k, y_k, z_k 是整数. 于是, 根据开始的讨论, 方程无解.

例18表明, 当 n 具有 $4^k(8l+7)$ 的形式时, 它不能表示成三个整数的平方和. 将整数表示成平方和是数论中最有趣的课题之一, 这方面的基本结果是:

任何正整数都能表示成四个整数的平方和. 当且仅当它不是 $4^k(8l+7)$ 这种形式时, 也能表示成三个整数的平方和.

我们已经看到, 同余能够卓有成效地证明某些方程无整数解. 或许有些读者期望它是证明方程无解的“万能方法”. 即猜测: 如果一个方程无整数解, 那么一定存在正整数 m, 使方程模 m 也无解. 然而答案是否定的, 请看例19.

例 19　证明：对任何正整数 m，方程

$$6xy-2x-3y+1\equiv 0 \pmod{m} \tag{33}$$

都有整数解 (x, y)，而不定方程

$$6xy-2x-3y+1=0 \tag{34}$$

无整数解.

证明　由 ㉞ 得 $(2x-1)(3y-1)=0$，从而它没有整数解（注意，它有实数解）.

另一方面，设 $m=2^{k-1}(2l-1)$，k，l 都是正整数．由于 $\dfrac{2^{2k+1}+1}{3}=2^{2k}-2^{2k-1}+\cdots+2-1$ 是整数，所以 $\left(l, \dfrac{2^{2k+1}+1}{3}\right)$ 就是 ㉝ 的整数解（$(2x-1)(3y-1)=(2l-1)\cdot 2^{2k+1}=2^{k+2}\cdot m$）.

例 19 表明，有这样的不定方程，它没有整数解，却不能用同余来证明．换一个等价的说法：同余方程 ② 对任何 m 都有整数解，并不能保证不定方程 ① 也有整数解.

另一方面，能够证明，对于一大类重要的不定方程，它们有整数解的充分必要条件，大致地说，是它有实数解并且同余式 ② 对任意 $m\geqslant 1$ 都有解．这是代数数论中很深刻的结果称为哈塞（Hasse）原理.

六、恒 等 式

我们已经看到，同余提供了一种证明方程无解的有效方法．本节的意图在于用恒等式来证明"几乎相反"的结论，即某些方程有整数解，以及有无穷多组整数解．这种论证的特色是构造性的，即通过恒等式直接找出一组或无穷多组解．然而作出与问题有关的恒等式通常并非易事，这要求解题者具有相当的灵活性，精于拼拼凑凑．

例 1　证明当 n 为奇数或 4 的倍数时，方程

$$x^2-y^2=n \qquad ①$$

有正整数解．

证明　众所熟知的恒等式

$$(k+1)^2-k^2=2k+1$$

表明当 n 为奇数 $2k+1$ 时，方程 ① 有解 $(k+1,\ k)$．

同样，恒等式

$$(k+1)^2-(k-1)^2=4k$$

表明当 $n=4k$ 时，① 有解 $(k+1,\ k-1)$．

例 1 可以帮助我们证明一些含有平方差的方程有解．

例 2　证明对任意整数 n，方程

$$x^2+y^2-z^2=n \qquad ②$$

有无穷多组整数解 $(x,\ y,\ z)$．

证明　将方程改写成

$$n-x^2=y^2-z^2.$$

选择与 n 具有相反奇偶性的 x(有无穷多个!)，则 $n-x^2$ 是奇数，问题可转化为例 1. 它恒可表示成平方差 y^2-z^2. 这就证明了方程 ② 有无穷多组解.

例 3 设 a 是给定的整数，证明方程

$$x^2+ay^2=z^2 \qquad ③$$

有无穷多组正整数解 (x, y, z).

证明 将方程改写成

$$ay^2=z^2-x^2.$$

只要取 y 与 a 有相同的奇偶性，则 ay^2 或者是奇数，或者被 4 整除，从而 ay^2 可写成平方差 z^2-x^2.

本题也可以直接利用恒等式

$$(m^2+an^2)^2-(m^2-an^2)^2=a(2mn)^2,$$

得出 $(m^2-an^2, 2mn, m^2+an^2)$ 是 ③ 的解.

另一种颇为有用的方法是先建立恒等式

$$(x_1^2+ay_1^2)(x_2^2+ay_2^2)=(x_1x_2\pm ay_1y_2)^2+a(x_1y_2\mp x_2y_1)^2 \qquad ④$$

这恒等式表明形如 x^2+ay^2 的数相乘，所得的积仍为同样的形式.

因此，如果 (x_1, y_1, z_1) 与 (x_2, y_2, z_2) 是 ③ 的解，那么由于平方数的积仍为平方数以及 ④，$(|x_1x_2\pm ay_1y_2|, |x_1y_2\mp x_2y_1|, z_1z_2)$ 也是 ③ 的解.

取 ③ 的一组正整数解（由 $(1+a)^2-(1-a)^2=a\times 2^2$，$(4+a)^2-(4-a)^2=a\times 4^2$ 等可知 $(|1-a|, 2, |1+a|)$ 或 $(|4-a|, 4, |4+a|)$ 是 ③ 的正整数解）(x_1, y_1, z_1)，然后反复应用上面的方法，就产生出 ③ 的无穷多组正整数解（如果 $x_1x_2-ay_1y_2=0$，则 $x_1x_2+ay_1y_2\neq 0$，并且 $x_1y_2-x_2y_1\neq 0$. 否则导出 $x_1^2=ay_1^2$，结合 ③ 得 $2x_1^2=z_1^2$，这当然是不可能的. 所以每一次产生的两组解中至少有一组正整数解）.

④ 不难验证，但我们更乐意提及它的一个背景。

数 $x_1+\sqrt{-a}y_1$（可能是虚数）与它的"共轭数" $x_1-\sqrt{-a}y_1$ 的积 $x_1^2+ay_1^2$ 称为 $x_1\pm\sqrt{-a}y_1$ 的范数．用两种不同的方法计算 $(x_1+\sqrt{-a}y_1)(x_2+\sqrt{-a}y_2)$ 的范数．

一方面，$(x_1+\sqrt{-a}y_1)(x_2+\sqrt{-a}y_2)=(x_1x_2-ay_1y_2)+\sqrt{-a}(x_1y_2+x_2y_1)$，所以它的范数为 $(x_1x_2-ay_1y_2)^2+a(x_1y_2+x_2y_1)^2$．另一方面，如果先取范数再相乘，便得到 $(x_1^2+ay_1^2)(x_2^2+ay_2^2)$．两个结果应当相同，这就导出 ④（我们已经闯进了数域 $Q(\sqrt{-a})$，即第三节末所说的，将 $\sqrt{-a}$ 与有理数加减乘除而得到的代数数域）．

特别地，在 ④ 中取 $a=1$，就有

$$(x_1^2+y_1^2)(x_2^2+y_2^2)=(x_1x_2\pm y_1y_2)^2+(x_1y_2\mp x_2y_1)^2, \qquad ⑤$$

即两个平方的和乘以两个平方的和，所得的积仍为两个平方的和．

⑤ 也有很多用处．

例 4　证明方程

$$x^2+y^2=z+z^5 \qquad ⑥$$

有无穷多组正整数解 (x, y, z)，并且 x、y 互素．

证明　取 $z=a^2+b^2$，则由 ⑤，

$$\begin{aligned} z+z^5=z(1+z^4)&=(a^2+b^2)(1+(z^2)^2)\\ &=(a+bz^2)^2+(az^2-b)^2. \end{aligned}$$

这样，取 $x=a+bz^2$，$y=az^2-b$，并且 $z=a^2+b^2$，就得到原方程的无穷多组正整数解（a, b 都是正整数）．

为了得到无穷多组满足 $(x, y)=1$ 的解，我们"退一步"来做到这一点．取 $b=1$（尝试！）．请注意，此时实际上是在上面已得的解中寻求使 $(x, y)=1$ 的充分条件（$b=1$ 并非必要）．下面来证，这样的 x, y 一定是互素的．因为

$$x=a+(a^2+1)^2,\ y=a(a^2+1)^2-1,$$

设 $d=(x, y)$，则 $d|ax-y$，即 $d|a^2+1$. 再从 $d|y$ 可知，$d|1$. 于是 $d=1$.

从而 $x=a+(a^2+1)^2$，$y=a(a^2+1)^2-1$，$z=a^2+1$ 便是方程满足 $(x, y)=1$ 的正整数解（a 是任意正整数），这自然有无穷多组.

例 5 试证明，对于任意给定的正整数 n，方程

$$x^2+y^2=z^n$$

有无穷多组整数解 (x, y, z)，且 $xy\neq 0$.

证明 利用 ⑤ 不难解决. 不过，我们宁愿直接用复数（实际上是 $Q(i)$ 中的数）来处理. 令 $w=a+bi$，这里 a、b 为两个互素的自然数. 我们用两种方法来计算 w^{2n} 的模.

首先，$w^n=x+yi$，由二项式定理易知 x、y 都是整数，均不为 0（$x=a^n-C_n^2a^{n-2}b^2+\cdots=0$ 导出 $b|a^n$；$y=0$ 导出 $a|b^n$，与 a、b 互素矛盾）.

我们有 $$|w^{2n}|=|w^n|^2=x^2+y^2,$$

又有 $$|w^{2n}|=(|w^2|)^n=(a^2+b^2)^n,$$

即 $$(a^2+b^2)^n=x^2+y^2.$$

因此，原方程有无穷多组整数解 (x, y, a^2+b^2)，其中 a、b 为互素自然数，$x=a^n-C_n^2a^{n-2}b^2+C_n^4a^{n-4}b^4-\cdots\neq 0$，$y=C_n^1a^{n-1}b-C_n^3a^{n-3}b^3+\cdots\neq 0$.

从这个例子可以看出，进入代数数域（如 $Q(i)$）是有帮助的.

为了证明方程有无穷多组解（请注意，我们的目的并不是求全部解），也可以先求出一组解，然后借助于适当的恒等式产生无穷多组解. 例 3 中（第二种解法）已经这样做过. 下面的例 6 也是如此.

例 6　证明方程

$$x^2+y^3=z^4$$

有无穷多组正整数解(x, y, z).

证明　我们先指出，如果方程有一组正整数解(x_0, y_0, z_0)，则它有无穷多组解．这只要注意恒等式

$$(x_0d^6)^2+(y_0d^4)^3=(z_0d^3)^4 \quad (d=1, 2, \cdots)$$

即可．

为了得到一组正整数解，可先取x为最小的自然数1，考察有无y，使1^2+y^3为平方数，易知

$$1^2+2^3=3^2,$$

两边同乘3^6(6是左边指数的公倍数，并且与右边指数2的和是4的倍数)得

$$3^6+3^6\cdot 2^3=3^8,$$

即

$$(3^3)^2+(3^2\cdot 2)^3=(3^2)^4.$$

这表明方程有一组解是$x=3^3$, $y=2\times 3^2$, $z=3^2$．证毕．

本例还有一种不必先求解的证法(见第七节的例1)．

下面的例7与第九节的费尔马大定理形成鲜明的对比．

例 7　对任意的正整数m, n, $(m, n)=1$，都有无穷多组正整数x, y, z，使

$$x^n+y^n=z^m. \qquad ⑦$$

证明　与例6类似，如果⑦有一组正整数解，那么

$$(d^mx)^n+(d^my)^n=(d^nz)^m,$$

即(d^mx, d^my, d^nz)也是⑦的解．

为了求⑦的一组解，我们取两个正整数a、b，记

$$c=a^n+b^n.$$

将上式两边同乘c^{kn}得(读者可与例6对比)

$$(ac^k)^n+(bc^k)^n=c^{kn+1}. \qquad ⑧$$

我们希望 $kn+1$ 为 m 的倍数．由于 $(m, n)=1$，根据第一节的裴蜀恒等式 ④，存在正整数 k，l，使得

$$lm-kn=1. \qquad ⑨$$

对这样的 k、l，取 $x=ac^k$，$y=bc^k$，$z=c^l$，则由 ⑧ 得

$$x^n+y^n=z^m.$$

这就给出了 ⑦ 的无穷多组解（即使不乘 c 的幂，由于 a、b 的任意性，我们已经得到无穷多组解．在 a、b 固定时，满足 ⑨ 的 k、l 仍有无穷多种选择，又给出无穷多组解）．

表一个数为若干个某种类型的数的和，是堆垒数论（加性数论）中感兴趣的问题．这里举两个例子．

我们知道，有无穷多个整数不能表示成三个整数的立方和（上节例 4），然而借助恒等式却不难证明下面的结论．

例 8　每个整数都能够写成五个整数的立方和．

证明　论证的出发点是下面的恒等式

$$6x=(x+1)^3+(x-1)^3+(-x)^3+(-x)^3, \qquad ⑩$$

于是，每个被 6 整除的整数都能表示成四个整数的立方和，当然更是五个整数的立方和（只要再补一个 0 即可）．

用一个简单的技巧就能将其他情况化为这种情形．将整数 n 按模 6 分类，共得到六种形式的数，我们逐一来证．

当 $n=6x+1$ 时，注意

$$6x+1=6x+1^3,$$

显然，此时的 n 是五个整数的立方和．再看等式：

$$6x+2=6(x-1)+2^3,\ 6x+3=6(x-4)+3^3,$$

$$6x+4=6(x+2)+(-2)^3,\ 6x+5=6(x-1)+1^3.$$

分别用 $x-1$，$x-4$，$x+2$，$x-1$ 代替 ⑩ 中的 x 即得结果．

另一个直截了当的证法是，注意 n^3-n 总是 6 的倍数，即

$\frac{n^3-n}{6}$ 是整数. 利用

$$n=6\cdot\frac{n-n^3}{6}+n^3,$$

以 $\frac{n-n^3}{6}$ 代替 ⑩ 中的 a 即可.

例 9 形如 $\frac{n(n+1)}{2}$ 的正整数称为三角数($n\geqslant1$). 它等于 $1+2+\cdots+n$. 证明：每个不等于1, 6的三角数都是三个三角数的和.

证明 这问题等价于：当 $n\neq1, 3$ 时，方程

$$x(x+1)+y(y+1)+z(z+1)=n(n+1)$$

有正整数解 (x, y, z).

我们把 n 按模 3 分类，来构造有关的恒等式. 即分别考虑 $n=3k(k>1)$, $3k+1(k\geqslant1)$ 及 $3k+2(k\geqslant0)$ 三种情况.

当 $n=3k$ 时，$n(n+1)=3k(3k+1)=9k^2+3k$ (k^2 和 k 的系数都大于 1, 便于拼凑)，得到

$$3k(3k+1)=2k(2k-1)+2k(2k+1)+k(k-1), \quad (k>1)$$

当 $n=3k+1$, $n=3k+2$ 时，类似的恒等式是：

$$(3k+1)(3k+2)=2k(2k+1)+(2k+1)(2k+2)+k(k+1), \quad (k\geqslant1)$$

$$(3k+2)(3k+3)=(2k+1)(2k+2)+(2k+1)(2k+2)+(k+1)(k+2). \quad (k\geqslant0)$$

很显然，上面三个式子中的右端三项都是正整数，这就证明了结论.

在数论中，人们很喜欢把平方数和三角数进行比较，而考虑类似的问题. 请读者查看一下第十节中的例 6,在那里，我们

证明了，有无穷多个平方数不能表示成三个正整数的平方和。

方程组也可以借助恒等式来证明它有无穷多组解。

例 10 证明有无穷多组正整数(x, y, z)，使得x, y, z中任两个的和都是平方数。

证明 问题即要证明方程组

$$x+y=a^2,\ y+z=b^2,\ z+x=c^2 \quad ⑪$$

有无穷多组正整数解。

由 ⑪ 得

$$x=\frac{a^2-b^2+c^2}{2},\ y=\frac{a^2+b^2-c^2}{2},\ z=\frac{b^2+c^2-a^2}{2}. \quad ⑫$$

$a^2-b^2+c^2$, $a^2+b^2-c^2$, $b^2+c^2-a^2$的奇偶性相同，只要a, b, c中两奇一偶（或全为偶数），则x, y, z全为整数。

我们取$a=2n+1$, $b=2n$, $c=2n-1(n\geqslant 3)$，相应地有

$$x=2n^2+1,\ y=2n^2+4n,\ z=2n^2-4n.$$

这就得出无穷多组正整数解。

实际上，可以证明更强的结论：有无穷多组正整数x, y, z，每两个的平方和都是平方数（第十节例 2）。

例 11 证明方程组

$$\begin{cases} x^2+y^2=z^2-1, \\ x^2-y^2=t^2-1 \end{cases} \quad ⑬$$

有无穷多组正整数解(x, y, z, t)。

证明 恒等式

$$(2n^2)^2\pm(2n)^2=(2n^2\pm1)^2-1$$

表明$(2n^2, 2n, 2n^2+1, 2n^2-1)$是 ⑬ 的解。

例 12 证明

$$\begin{cases} x^2+y^2=z^2+1, \\ x^2-y^2=t^2+1 \end{cases} \quad ⑭$$

有无穷多组正整数解.

证明 对任意正整数 k, 我们有

$$(8k^4+1)^2\pm(8k^3)^2=(4k^2(2k^2\pm1))^2+1,$$

所以 $(8k^4+1,\ 8k^3,\ 4k^2(2k^2+1),\ 4k^2(2k^2-1))$ 是 ⑭ 的解.

注意从 ⑬、⑭ 中去掉 -1 或 $+1$ 后的方程组

$$\begin{cases}x^2+y^2=z^2,\\ x^2-y^2=t^2\end{cases}$$

没有正整数解, 证明见第九节例 4.

七、佩尔方程

许许多多的数论问题都归结到本节将要介绍的、形如

$$x^2-dy^2=1 \quad ①$$

的二元二次不定方程，其中 d 是整数．这种方程习惯上称为佩尔(Pell)方程(其实和佩尔毫无关系)．显然，当 $d<0$ 时，或者当 $d>0$ 但 d 是一个完全平方时，方程①只有平凡解 $(x, y)=(1, 0), (-1, 0)$．因此我们以下只考虑 $d>0$ 且不是完全平方数的情形(不再一一申明)．

用稍稍深入的方法(限于篇幅，本书不予证明)能够证明下面的基本结果．

定理1 方程①一定有正整数解．

下面来谈谈方程①的全部正整数解的求法．设 $x_1>0$，$y_1>0$ 是①的所有正整数解中使 $x_1-\sqrt{d}\,y_1$ 最小的一组解，则称 (x_1, y_1) 是方程的最小解．这时，对①的任一组正整数解 (x, y)，必有 $x_1\leqslant x$, $y_1\leqslant y$．先证明 $x_1\leqslant x$．否则的话，从 $x_1>x$ 以及 $x_1^2=dy_1^2+1$, $x^2=dy^2+1$ 可得 $dy_1^2+1>dy^2+1$，即 $y_1>y$，于是

$$x+y\sqrt{d}<x_1+y_1\sqrt{d},$$

和 (x_1, y_1) 的选取矛盾．同理 $y_1\leqslant y$．所以最小解就是①的一组正整数解 (x, y)，其中 x 与 y 均为最小．

最小解的另一个名称叫“基本解”．其来源在于由它能够“生成”①的全部整数解(因此是基本的)．这就是下面的又一

个基本结论.

定理2 方程①有无穷多组正整数解. 并且，全部正整数解(x, y)由

$$\begin{cases} x_n=\dfrac{1}{2}\left[(x_1+\sqrt{d}\,y_1)^n+(x_1-\sqrt{d}\,y_1)^n\right], \\ y_n=\dfrac{1}{2\sqrt{d}}\left[(x_1+\sqrt{d}\,y_1)^n-(x_1-\sqrt{d}\,y_1)^n\right] \end{cases} \quad ②$$

给出. 其中(x_1, y_1)是①的最小解，n为自然数.

定理2的证明在常见的数论书中均能找到，我们不再赘述.

最小解可以用尝试法定出. 例如令$y=1, 2, \cdots$直至dy^2+1成为完全平方(设为x^2)，这时(x, y)就是最小解. 但有些最小解也大得惊人. 例如

$$x^2-991y^2=1$$

的最小解是

$$x=379516400906811930638014896080,$$

$$y=12055735790331359447442538767.$$

在数论中，可以借助于连分数来求最小解，然而冗长的计算通常还是难免的.

公式②也可以写成

$$x_n+y_n\sqrt{d}=(x_1+y_1\sqrt{d})^n. \quad ③$$

公式②、③在实际求解时并不方便. 因此，我们设法导出正整数解的递推公式. 由③得

$$\begin{aligned} x_{n+1}+y_{n+1}\sqrt{d}&=(x_1+y_1\sqrt{d})^n(x_1+y_1\sqrt{d}) \\ &=(x_n+y_n\sqrt{d})(x_1+y_1\sqrt{d}), \end{aligned} \quad ④$$

将④的右端展开，与左端比较，便得

$$\begin{cases} x_{n+1}=x_1x_n+dy_1y_n, & ⑤ \\ y_{n+1}=x_1y_n+y_1x_n. & ⑥ \end{cases}$$

进一步还可导出数列$\{x_n\}$，$\{y_n\}$各自的递推公式．这只需在⑤中用$n-1$代替n，得

$$x_n=x_1x_{n-1}+dy_1y_{n-1}, \quad ⑦$$

从⑤中减去$x_1\times$⑦，注意到$x_1^2-dy_1^2=1$及⑥，便有

$$\begin{aligned}x_{n+1}&=2x_1x_n-x_1^2x_{n-1}+dy_1(y_n-x_1y_{n-1})\\&=2x_1x_n-x_1^2x_{n-1}+dy_1^2x_{n-1}=2x_1x_n-x_{n-1}.\end{aligned} \quad ⑧$$

同样，

$$y_{n+1}=2x_1y_n-y_{n-1}. \quad ⑨$$

有趣的是，递推公式⑧、⑨完全相同．

佩尔方程的理论问题已由定理1、2解决．我们将重点放在它的应用上．

例1 证明方程

$$x^2+y^3=z^4 \quad ⑩$$

有无穷多组正整数解．

证明 注意恒等式

$$\left(\frac{n(n-1)}{2}\right)^2+n^3=\left(\frac{n(n+1)}{2}\right)^2$$

（这恒等式不难验证．熟悉自然数立方和的读者一定看出它就相当于$1^3+2^3+\cdots+n^3=\left(\frac{n(n+1)}{2}\right)^2$）．它给出方程

$$x^2+y^3=u^2$$

的无穷多组正整数解$\left(\frac{n(n-1)}{2},\ n,\ \frac{n(n+1)}{2}\right)$．对于方程⑩，我们只要选择$n$，使得$\frac{n(n+1)}{2}$为完全平方．考察方程

$$n(n+1)=2k^2, \quad ⑪$$

它可以变形为

$$(2n+1)^2-2\cdot(2k)^2=1. \quad ⑫$$

我们知道佩尔方程

$$x^2-2y^2=1 \qquad ⑬$$

有无穷多组正整数解(x, y)，并且由于⑬的特点，x一定是奇数．模4可知，y一定是偶数．于是，令

$$n=\frac{x-1}{2},\ k=\frac{y}{2},$$

就由⑬的一组解得到⑪的一组解．从而⑪，⑩都有无穷多组正整数解．

不难算出⑬的最小解为$(3, 2)$．利用递推公式

$$x_{m+1}=6x_m-x_{m-1},\ y_{m+1}=6y_m-y_{m-1} \qquad ⑭$$

及初始条件$(x_0, y_0)=(1, 0)$，$(x_1, y_1)=(3, 2)$可算出解

$$(17, 12),\ (99, 70),\ (577, 408),\ \cdots$$

相应的$n=8, 49, 288, \cdots$．从而有

$$28^2+8^3=6^4,$$

$$1176^2+49^3=35^4,$$

$$41328^2+288^3=204^4,$$

$$\cdots\cdots$$

这类"数的奇观"的背后，往往隐藏着佩尔方程．

例2 求出所有为完全平方数的三角数．

解 问题等价于确定满足方程

$$n(n+1)=2k^2\ (k\text{是正整数}) \qquad ⑪$$

的全部正整数n．这已在例1中解决．由递推公式⑭立即导出n，k的递推公式为

$$\begin{cases} n_m=6n_{m-1}-n_{m-2}+2, \\ k_m=6k_{m-1}-k_{m-2}. \end{cases}$$

$n_1=1$，$k_1=1$；$n_2=8$，$k_2=6$．不难算出前几对(k, n)是

$$(1, 1),\ (6, 8),\ (35, 49),\ (204, 288),\ (1189, 1681),\ \cdots.$$

在第十节例8中，我们将证明大于1的三角数不可能是整数的四次方.

下面是一个关于整边三角形的问题，实际上这也是佩尔方程的应用.

例3 三角形的边长分别是 $a-1$, a, $a+1$, h 表示 a 边上的高，三角形面积记为 S，其中 a, h, S 是正整数. 证明：满足这些条件的全部三数组 $(a, h, S)=(a_n, h_n, S_n)$ 由下面的递推公式确定 $(n\geqslant1)$：

$$\begin{cases}a_{n+2}=4a_{n+1}-a_n,\\ h_{n+2}=4h_{n+1}-h_n,\\ S_{n+2}=14S_{n+1}-S_n,\end{cases}$$

而
$$(a_1, h_1, S_1)=(4, 3, 6),$$
$$(a_2, h_2, S_2)=(14, 12, 84).$$

证明 用两种方法计算面积 S. 首先，

$$S=\frac{1}{2}ah;$$

又由海伦公式，

$$S=\sqrt{\frac{1}{2}(3a)\times\frac{1}{2}(a+2)\times\frac{1}{2}a\times\frac{1}{2}(a-2)}$$
$$=\frac{1}{4}a\sqrt{3a^2-12}.$$

由于 S 是整数，所以 $3a^2-12$ 是完全平方，并且 a 是偶数(否则的话，$3a^2-12$ 是奇数的平方，从而 $a\sqrt{3a^2-12}$ 是奇数).

设
$$a=2x,$$
则
$$S=hx,\ h^2=3(x^2-1).$$
于是有，$3\mid h^2$，但3是素数，故 $3\mid h$.

设
$$h=3y,$$
便有
$$S=3xy,$$

及

$$x^2-3y^2=1.\qquad ⑮$$

我们的问题化为求佩尔方程⑮的所有正整数解 (x_n, y_n). 由公式⑧, ⑨知

$$\begin{cases} x_{n+2}=4x_{n+1}-x_n, \\ y_{n+2}=4y_{n+1}-y_n. \end{cases}$$

这里 $x_0=1$, $y_0=0$, $x_1=2$, $y_1=1$. 从而 $x_2=7$, $y_2=4$. 又 $a_n=2x_n$, $b_n=3y_n$, 所以

$$\begin{cases} a_{n+2}=4a_{n+1}-a_n, \\ b_{n+2}=4b_{n+1}-b_n, \end{cases}$$

其中 $(a_1, b_1)=(4, 3)$, $(a_2, b_2)=(14, 12)$.

剩下的是证明

$$S_{n+2}=14S_{n+1}-S_n.\qquad ⑯$$

首先注意

$$x_{2n}+y_{2n}\sqrt{3}=(2+\sqrt{3})^{2n}$$
$$=((2+\sqrt{3})^n)^2=(x_n+y_n\sqrt{3})^2$$

将上式右边展开, 并与左边比较得

$$y_{2n}=2x_ny_n=\frac{2}{3}S_n.\qquad ⑰$$

因此问题就是求 $\{y_{2n}\}$ 的递推公式. 由于

$$x_{2n}+y_{2n}\sqrt{3}=(2+\sqrt{3})^{2n}=(7+4\sqrt{3})^n$$

所以由⑨得(那里的下标均乘2, 而 $2x_2=2\times 7=14$)

$$y_{2n+2}=14y_{2n}-y_{2n-2}.$$

从而由⑰得出⑯, 并且

$$S_1=\frac{3y_2}{2}=\frac{3\times 4}{2}=6,\ \ S_2=84\ (S_0=y_0=0).$$

例 4　证明不定方程

$$5^a-3^b=2 \tag{18}$$

仅有的正整数解是 $a=b=1$.

证明　显然,当 a、b 中有一个为 1 时,另一个也为 1. 设 $a>1$, $b>1$. ⑱模 4,得

$$1^a-(-1)^b\equiv 2(\bmod 4),$$

即
$$(-1)^b\equiv -1(\bmod 4),$$

从而 b 是奇数. 进一步模 3,有

$$(-1)^a\equiv 2(\bmod 3),$$

表明 a 也是奇数.

设 $u=3^b+1$, $v=3^{\frac{b-1}{2}}\cdot 5^{\frac{a-1}{2}}$, 则有

$$15v^2=3^b\cdot 5^a=3^b(3^b+2)=(3^b+1)^2-1$$
$$=u^2-1,$$

因此 $x=u$, $y=v$ 是佩尔方程

$$x^2-15y^2=1 \tag{19}$$

的一组正整数解.

⑲的最小解是 $x_1=4$, $y_1=1$. 设其全部解为 (x_n, y_n), 则 $\{y_n\}$ 满足(用公式⑨)

$$y_n=8y_{n-1}-y_{n-2}\quad (n\geqslant 3), \tag{20}$$
$$y_1=1,\ y_2=8.$$

我们证明 $\{y_n\}$ 中不可能有形如 $3^\alpha\cdot 5^\beta$ (α、β 为正整数)的项,从而导致矛盾. 为此,先将数列 $\{y_n\}$ 模 3,成为

$$1,\ 2,\ 0,\ 1,\ 2,\ 0,\ 1,\ 2,\ 0,\ \cdots$$

即当且仅当 $3|n$ 时,有 $3|y_n$.

再将 $\{y_n\}$ 模 7 成为

$$1,\ 1,\ 0,\ -1,\ -1,\ 0,\ 1,\ 1,\ 0,\ -1,\ -1,\ 0,\ \cdots$$

即当且仅当 $3|n$ 时有 $7|y_n$. 这样便推出"$3|y_n\Leftrightarrow 7|y_n$". 于

法，含有因数3而不含因数7的数$3^a\cdot5^b$不在数列$\{y_n\}$中出现．⑱仅有一组整数解$a=b=1$．

形如

$$x^2-dy^2=-1 \tag{21}$$

的方程也称为佩尔方程．这里$d>0$且不是平方数．它和方程①形式上相差甚小，但解的情况却很不相同．例如，当$d\equiv3 \pmod 4$时，不难用同余证明㉑没有整数解．当然，也有无穷多个d使方程㉑有正整数解(见习题28)．要确定所有使㉑有整数解的d并非一件容易的事．

与定理1、2类似，对于㉑有以下结论．

定理3 设$d>0$不是完全平方数，如果方程㉑有正整数解，则必有无穷多组．设$x_1+y_1\sqrt{d}$是所有$x>0$，$y>0$的解中使$x+y\sqrt{d}$最小的那组解（(a, b)称为㉑的最小解），则由$(x_1+y_1\sqrt{d})^2=u_1+v_1\sqrt{d}$决定的$(u_1, v_1)$是$x^2-dy^2=1$的最小解．并且方程㉑的全部正整数解$(x, y)$由

$$x_n+y_n\sqrt{d}=(x_1+y_1\sqrt{d})^{2n+1} \tag{22}$$

给出$(n\geqslant0)$．

这定理的证明可参阅柯召和孙琦的《谈谈不定方程》第二章．

下面这道例题有多种解法．我们利用佩尔方程的理论来解．

例5 设$a_n=[\sqrt{n^2+(n+1)^2}]\ (n\geqslant1)$，这里$[x]$表示$x$的整数部分，证明：

(i) 有无穷多个n，使得$a_{n+1}-a_n>1$．

(ii) 有无穷多个n，使得$a_{n+1}-a_n=1$．

证明 不难看出(i)和(ii)至少有一个是正确的．但要证

明两者都对无穷多个 n 成立就不那么容易了.

考虑佩尔方程

$$x^2-2y^2=-1. \quad ㉓$$

$(1, 1)$显然是它的最小解. 因此, 由定理 3, ㉓ 有无穷多组正整数解(x, y). 又 x 必为奇数, 设 $x=2n+1$, 代入㉓, 化简得

$$n^2+(n+1)^2=y^2, \quad ㉔$$

因此有无穷多个正整数 n, 使㉔成立.

为了证明(i), 取 n 满足㉔, 则 $a_n=y$, 而

$$a_{n-1}=[\sqrt{(n-1)^2+n^2}]=[\sqrt{y^2-4n}].$$

由㉔显然有 $y\leqslant 2n$, 所以

$$\sqrt{y^2-4n}<y-1,$$

于是

$$a_{n-1}<y-1,$$

即

$$a_n-a_{n-1}>1,$$

这就证明了(i).

对于(ii), 仍取 n 满足㉔, $a_n=y$, 这时,

$$a_{n+1}=[\sqrt{(n+1)^2+(n+2)^2}]=[\sqrt{y^2+4n+4}].$$

从㉔式不难推出

$$n<y\leqslant 2n+1,$$

即

$$2y+1<4n+4<4y+4,$$

所以

$$y+1<\sqrt{y^2+4n+4}<y+2,$$

于是

$$a_{n+1}=[\sqrt{y^2+4n+4}]=y+1,$$

即

$$a_{n+1}-a_n=1,$$

这就证明了(ii).

例 6 求出所有的正整数 k, l, 使得

$$1+2+\cdots+k=(k+1)+(k+2)+\cdots+l.$$

解 将问题中的等式两边同加 $1+2+\cdots+k$, 变形为

$$2k(k+1)=l(l+1),$$

即

$$(2l+1)^2-2(2k+1)^2=-1.\quad ㉕$$

令 $x=2l+1$, $y=2k+1$, 则又一次得到佩尔方程

$$x^2-2y^2=-1.\quad ㉓$$

例5中已经说过 x 是奇数，由等价的㉔看出 y 也是奇数．所以㉕与㉓是一致的．由定理3，㉓的全部整数解由

$$x+y\sqrt{2}=(1+\sqrt{2})^{2n+1}\quad (n\geqslant 1)$$

给出．即 $x=\frac{1}{2}((1+\sqrt{2})^{2n+1}+(1-\sqrt{2})^{2n+1})$,

$$y=\frac{1}{2\sqrt{2}}((1+\sqrt{2})^{2n+1}-(1-\sqrt{2})^{2n+1}).\quad (n\geqslant 1)$$

于是相应的 $(k_n,\ l_n)=\left(\frac{y_n-1}{2},\ \frac{x_n-1}{2}\right)$ 由

$$k_n=\frac{1}{4\sqrt{2}}((1+\sqrt{2})^{2n+1}-(1-\sqrt{2})^{2n+1})-\frac{1}{2},$$

$$l_n=\frac{1}{4}((1+\sqrt{2})^{2n+1}+(1-\sqrt{2})^{2n+1})-\frac{1}{2}\ (n\geqslant 1)$$

给出．

公式㉒在数值计算时并不方便．更为实用的是与⑧、⑨类似的递推公式，为了导出这种公式，首先注意

$$(x_1+y_1\sqrt{d})^{2n}=(u_1+v_1\sqrt{d})^n=u_n+v_n\sqrt{d},$$

这里 $(u_n,\ v_n)$ 是

$$x^2-dy^2=1\quad ①$$

的正整数解．$(u_1,\ v_1)$ 是①的最小解．所以

$$u_n=2u_1u_{n-1}-u_{n-2},\quad ㉖$$

$$v_n=2u_1v_{n-1}-v_{n-2}.\quad ㉗$$

而 $x_n+y_n\sqrt{d}=(x_1+y_1\sqrt{d})^{2n+1}$

$$=(x_1+y_1\sqrt{d})(u_n+v_n\sqrt{d}),$$

所以 $x_n=x_1u_n+dy_1v_n$.

由于㉖、㉗是形式完全相同的一次式，立即得出递推公式

$$x_n = 2u_1 x_{n-1} - x_{n-2}. \qquad ㉘$$

同样，

$$y_n = 2u_1 y_{n-1} - y_{n-2}, \qquad ㉙$$

其中 $u_1 = x_1^2 + dy_1^2 = 2x_1^2 + 1$.

例 6 中的 k_n, l_n 也都以㉙为递推公式（取 $u_1 = 3$）.

最后，我们简单地谈谈一般形式的佩尔方程

$$x^2 - dy^2 = c. \qquad ㉚$$

这里 $d>0$ 不是完全平方，$c\neq 0$ 是整数. 它比①及㉓要复杂得多. 例如，当 $c\equiv d\equiv -1 \pmod 4$ 时，方程㉚没有整数解. 下面的定理 4 反映了佩尔方程的共性.

定理 4 如果方程㉚有一组正整数解 (a, b)，则它有无穷多组正整数解. 并且，设 (u, v) 是①的正整数解，则由

$$x + y\sqrt{d} = (a + b\sqrt{d})(u + v\sqrt{d}) \qquad ㉛$$

确定的正整数 (x, y) 都是㉚的解.

证明 由㉛取共轭得

$$x - y\sqrt{d} = (a - b\sqrt{d})(u - v\sqrt{d}) \qquad ㉜$$

㉛、㉜两式相乘即得

$$x^2 - dy^2 = (a^2 - db^2)(u^2 - dv^2) = a^2 - db^2 = c.$$

一般说来，㉛或者等价的公式

$$x_n + y_n\sqrt{d} = (a + b\sqrt{d})(u_1 + v_1\sqrt{d})^n \qquad ㉝$$

（(u_1, v_1) 为①的最小解）并不能给出㉚的全部正整数解. 求其全部解的方法请参阅柯召、孙琦的《谈谈不定方程》第二章.

一般的二元二次不定方程

$$ax^2 + bxy + cy^2 + dx + ey + f = 0 \qquad ㉞$$

（a、b、c、d、e、f 为整数）的求解可以归结为佩尔方程㉚. 有兴

趣的读者请参阅华罗庚的《数论导引》第十一章. 这里仅举一个简单的例子.

例 7 设 $k>1$ 是给定的整数, 证明有无穷多个整数 n, 使得 $kn+1$ 及 $(k+1)n+1$ 都是完全平方.

证明 考虑方程组

$$\begin{cases} kn+1=u^2, & ㉟ \\ (k+1)n+1=v^2. & ㊱ \end{cases}$$

消去 n, ㉟ $\times(k+1)-$ ㊱ $\times k$, 得

$$(k+1)u^2-kv^2=1. \quad ㊲$$

注意对㊲的任一组正整数解 (u, v), 取 $n=v^2-u^2$, 则易知 n 适合㉟, ㊱. 因此我们证明方程㊲有无穷多组正整数解即可. 由㊲, 作代换

$$\begin{cases} x=(k+1)u-kv, \\ y=v-u, \end{cases} \quad ㊳$$

则得出有无穷多组正整数解的佩尔方程

$$x^2-k(k+1)y^2=1. \quad ㊴$$

由㊳解得

$$\begin{cases} u=x+ky, \\ v=x+(k+1)y, \end{cases} \quad ㊵$$

因此方程㊲有无穷多组正整数解. 从而方程组㉟, ㊱均有无穷多组正整数解(而且根据定理 2, 可以全部求出来).

八、勾 股 数

勾股数是不定方程中最有趣的内容．所谓勾股数，用几何语言来说，就是勾股三角形（边长为整数的直角三角形）的三条边长；或者说是不定方程

$$x^2+y^2=z^2 \quad ①$$

的一组正整数解(x, y, z)．不难写出

$$3^2+4^2=5^2,$$
$$6^2+8^2=10^2,$$
$$5^2+12^2=13^2.$$

容易证明，方程①有无穷多组正整数解．例如在第六节例3中取$a=1$即可得知．在求①的全部正整数解之前，请先看它们的一个算术性质．

例 1　设(x, y, z)是方程①的任意一组正整数解，则有$60|xyz$．

证明　注意$60=3\times4\times5$，且3，4，5两两互素．我们只要证明xyz分别被3，4，5整除，就可推出$60|xyz$．

①模3．易知$x^2, y^2, z^2\equiv0, 1 \pmod 3$．它们不能都$\equiv1 \pmod 3$，否则①就给出$2\equiv1 \pmod 3$，矛盾．从而其中必有一个，不妨设为$x^2$，使得$x^2\equiv0 \pmod 3$，即$3|x^2$．因3是素数，这就推出$3|x$，于是$3|xyz$．

同样，①模5，$x^2, y^2, z^2\equiv0, \pm1 \pmod 5$．如果它们都不被5整除，则①的左边$\equiv0, \pm2 \pmod 5$，右边$\equiv\pm1 \pmod 5$，

这显然不可能．所以$5|x^2y^2z^2$，即$5|xyz$（注意5是素数）．

由①可知，x, y, z中必有一个是偶数．如果至少有两个偶数，则显然$4|xyz$．

如果恰有一个偶数，则$2\nmid z$，否则①模4将得到$2\equiv 0 \pmod 4$，这不可能．于是x, y一奇一偶．不妨设$2|y$．①再模8，有
$$1+y^2\equiv 1 \pmod 8,$$
即$8|y^2$，所以y必是4的倍数．故$4|xyz$．证毕．

由方程①不难看到，如果$(x, y)=d$，则$d^2|z^2$，即$d|z$，这样可在①的两边约去d^2．所以讨论①的解时，我们可以设$(x, y)=1$．容易得知，此时x, y, z实际上是两两互素的．这种x, y, z两两互素的勾股数(x, y, z)，称为①的*本原解*或*本原的勾股数*，相应的勾股三角形则称为*本原的勾股三角形*．由于$(x, y)=1$，从例1的解答过程可知，这时x, y一奇一偶．不妨设y为偶数．下面我们来求出①的全部本原解．它在勾股数的理论中扮演着基本的角色．

定理 不定方程①满足
$$(x, y)=1,\ x>0,\ y>0,\ z>0,\ 2|y \qquad ②$$
的全部整数解(x, y, z)可表示成
$$x=a^2-b^2,\ y=2ab,\ z=a^2+b^2. \qquad ③$$
其中a, b是满足

$a>b>0$，a, b一奇一偶，且$(a, b)=1$的任意整数．

证明 定理的内容包含两个部分．其一是，当a, b适合上述要求时，由③给出的(x, y, z)是方程①的解且满足②；其二是，对于①的任一组满足②的解(x, y, z)，一定可以找到适合定理中要求的整数a, b，使得x, y, z能表示成③的形式．

因为
$$(a^2-b^2)^2+(2ab)^2=(a^2+b^2)^2,$$
故由③给出的(x, y, z)是①的解．显然$x>0$，$y>0$，$z>0$．

还需证明这是一组本原解，即适合$(x, y)=1$，且$2|y$.

$2|y$是明显的．我们来证$(x, y)=1$．设$(x, y)=d$，则$d|x$，$d|z$，即$d|(a^2-b^2)$，$d|(a^2+b^2)$．从而$d|2a^2$，$d|2b^2$，推出$d|2(a^2, b^2)$．因为$(a, b)=1$，所以$(a^2, b^2)=1$，这就得到$d|2$．但a，b一奇一偶，这意味着$x=a^2-b^2$为奇数．从而$d=1$.

反过来，设(x, y, z)是①的任意一组满足②的解．因y为偶数，x，z为奇数，故$\frac{z-x}{2}$，$\frac{z+x}{2}$都是整数，并且有

$$\left(\frac{z-x}{2}, \frac{z+x}{2}\right)=\left(\frac{z-x}{2}+\frac{z+x}{2}, 2\cdot\frac{z+x}{2}\right)$$
$$=(z, z+x)=(z, x)=1.$$

由①得
$$\frac{z-x}{2}\cdot\frac{z+x}{2}=\left(\frac{y}{2}\right)^2,$$

所以$\frac{z-x}{2}$和$\frac{z+x}{2}$都是完全平方数．即有整数$a>b>0$，$(a, b)=1$，使得

$$\frac{z+x}{2}=a^2, \quad \frac{z-x}{2}=b^2, \quad y=2ab.$$

这时显然有　$x=a^2-b^2$，$y=2ab$，$z=a^2+b^2$.

又因为z为奇数，故a，b一奇一偶，证毕．

如果方程①的正整数解(x, y, z)不满足$(x, y)=1$，即非本原解．我们设$(x, y)=d$，$d>1$．则

$$\left(\frac{x}{d}, \frac{y}{d}\right)=1,$$

且$\left(\frac{x}{d}, \frac{y}{d}, \frac{z}{d}\right)$是①的本原解．利用以上定理可知，存在整数$a>b>0$，$(a, b)=1$，且$a$，$b$一奇一偶，使$\left(我们设2\left|\frac{y}{d}\right.\right)$

$$x=(a^2-b^2)d, \quad y=2abd, \quad z=(a^2+b^2)d. \qquad ④$$

应用定理，不难列出前11个本原的勾股三角形(x, y, z)（以a的大小为序）为：

a	b	x	y	z	面积
2	1	3	4	5	6
3	2	5	12	13	30
4	1	15	8	17	60
4	3	7	24	25	84
5	2	21	20	29	210
5	4	9	40	41	180
6	1	35	12	37	210
6	5	11	60	61	330
7	2	45	28	53	630
7	4	33	56	65	924
7	6	13	84	85	546

我们看到3, 4, 5, 7, 8, 9, 11, 12, 13, 15, 16, 17, …都出现在上面的表格中．这意味着，一定有本原的勾股三角形，它的某条边长是这些数．自然，我们希望确定哪些数能够出现在一组本原勾股数中，即对怎样的n，存在（至少一个）本原的勾股三角形，其一条边长为n．

例2 设$n>2$，则n出现在一组本原勾股数中的充分必要条件是$n \not\equiv 2 \pmod 4$．

证明 先证明条件是充分的．如果n是奇数，恒等式

$$n^2+\left(\frac{n^2-1}{2}\right)^2=\left(\frac{n^2+1}{2}\right)^2$$

表明$\left(n, \frac{n^2-1}{2}, \frac{n^2+1}{2}\right)$是一组勾股数．它显然是本原的，因为$\frac{n^2-1}{2}$与$\frac{n^2+1}{2}$的差为1，当然互素．

同样，当 n 为偶数时，有恒等式

$$n^2+\left(\frac{n^2}{4}-1\right)^2=\left(\frac{n^2}{4}+1\right)^2. \quad (n>2)$$

因为 $n\not\equiv 2 \pmod 4$，所以 $4|n$，$\frac{n^2}{4}$ 是偶数，$\frac{n^2}{4}-1$ 与 $\frac{n^2}{4}+1$ 是相邻的奇数，它们互素。

这样，我们作出了一组出现 n 的本原勾股数。

再证明条件是必要的。由例 1，$4|xyz$，所以本原勾股数 x、y、z 中唯一的偶数被 4 整除，x、y、z 均 $\not\equiv 2 \pmod 4$。

从上面的证明不难看出，每个整数 $n>2$ 都出现在一组勾股数中(未必本原)。有些正整数能够出现在许多组勾股数中。对每个 $n>2$，确定它在多少组勾股数中出现，则是一个复杂的问题，然而我们却能比较容易地给出下面的结论。

例 3 证明对任何给定的非负整数 k，都存在正整数 n，它恰好在 k 组勾股数中出现。

这里给出的两种证法都是构造性的。

证法一 我们证明，对 $k\geq 0$，$n=2^{k+1}$ 恰好在 k 组勾股数中出现。采用归纳法。当 $k=0$ 时，$2^1=2$ 不在任何勾股数中出现，结论成立。假定对于非负整数 $k-1$ 结论成立，即 2^k 恰好出现在 $k-1$ 组勾股数中。由此，将每组中的三个数都扩大两倍，产生出 $k-1$ 组(非本原)勾股数，每一组中都包含 2^{k+1}。反过来，如果 2^{k+1} 出现在一组非本原的勾股数中，则其中各数都是偶数，约去 2 得出一组出现 2^k 的勾股数。所以(由归纳假设)2^{k+1} 恰在 $k-1$ 组非本原的勾股数中出现。

但 2^{k+1} 恰好在一组本原的勾股数中出现。这是因为 $k\geq 1$，所以 $4|2^{k+1}$，故 2^{k+1} 必在一组本原的勾股数中出现(例 2)。又由定理可知，对出现 2^{k+1} 的本原的勾股数(x, y, z)，存在整数

$a>b>0$, $(a, b)=1$ 且 a, b 一奇一偶, 使得

$$x=a^2-b^2,\ y=2ab,\ z=a^2+b^2.$$

这仅可能 $y=2ab=2^{k+1}$, 从而 $a=2^{k+2}$, $b=1$. 这样, 2^{k+1} 仅能在一组本原的勾股数中出现. 连同上面已得到的 $k-1$ 组(非本原)的勾股数, 可知 2^{k+1} 恰在 k 组勾股数中出现. 证毕.

证法二　设 p 是 $4m-3$ 型的素数. 下面来证明, p^k 恰好在 k 组勾股数中出现. 选择 $p\equiv 3 \pmod 4$, 并不是我们偏爱这种形式的素数. 而是因为由第九节例 1 可以知道, 这种 p 的方幂决不能是两个正整数的平方和, 从而它不会成为一组勾股数中最大的数. 因此, 假设 p^k 是勾股数中的一个数, 则有正整数 $z>y$ (勾股数组中的另两个数), 使得

$$(z-y)(z+y)=p^{2k}.$$

所以对于某个 $m\in\{0, 1, \cdots, k-1\}$, 有(注意 p 是素数!)

$$z-y=p^m,\ z+y=p^{2k-m}.$$

反过来, 每个这样的 m 对应于一组解, 所以, 恰好有 k 组勾股数含有 p^k, 即取

$$x=p^k,\ y=\frac{1}{2}(p^{2k-m}-p^m),\ z=\frac{1}{2}(p^{2k-m}+p^m).$$

其中 $m=0, 1, \cdots, k-1$.

可以证明形如 $4m+3$ 状的素数有无穷多个. 这样, 证法二表明了具有问题中所说性质的 n 有无穷多个.

不难看出, 边长为连续整数的勾股三角形只有一个, 即 $(3, 4, 5)$. 但斜边和一条直角边为连续整数的勾股三角形却有无穷多个. 我们能把这样的三角形都确定出来.

例 4　确定所有的斜边与一条直角边为连续整数的勾股三角形.

解　问题等价于求出方程

$$x^2+y^2=z^2$$

的满足 $z=y+1$ 或者 $z=x+1$ 的全部正整数解 (x, y, z).

由于 x 和 y 的位置是对称的，我们不妨设 $z=y+1$. 由

$$x^2=z^2-y^2=(y+1)^2-y^2=2y+1$$

得出 x 为奇数. 设 $x=2b+1$, 则

$$y=2b(b+1),\ z=2b^2+2b+1,$$

这里 b 为任意正整数.

两直角边是连续整数的勾股三角形也有无穷多个，它们的全部解和佩尔方程紧密相关.

例 5 求出所有直角边为连续整数的勾股三角形.

解 设这样的三角形三边为 x, $y=x+1$, z. 则问题等价于求出方程

$$x^2+(x+1)^2=z^2 \qquad ⑤$$

的全部正整数解 (x, z).

这方程就是第七节中的㉔，它可以化为佩尔方程

$$(2x+1)^2-2z^2=-1,$$

从而可以利用第七节的递推公式㉕、㉖(其中 $a_1=6$). 用 $2x_n+1$ 代替公式中的 x_n. 稍作化简便得

$$\begin{cases} x_{n+1}=6x_n-x_{n-1}+2, \\ z_{n+1}=6z_n-z_{n-1}, \end{cases}$$

其中 $x_0=0$, $z_0=1$, $x_1=3$, $z_1=5$. 用递推公式不难列出前几个这样的三角形为

n	x	y	z
1	3	4	5
2	20	21	29
3	119	120	169
4	696	697	985
5	4059	4060	5741

由例 5 可知，有无穷多个勾股三角形其面积是三角数．显然也有无穷多个三角数是完全平方．然而，勾股三角形的面积却不能是完全平方(见第九节例 2)．

此外，现在容易推出，有无穷多个勾股三角形，两条直角边都是三角数．因为从

$$x^2+(x+1)^2=z^2,$$

便有 $(x(2x+1))^2+((2x+1)(x+1))^2=(z(2x+1))^2,$

即 $\left(\frac{2x(2x+1)}{2}\right)^2+\left(\frac{(2x+1)(2x+2)}{2}\right)^2=(z(2x+1))^2.$

甚至有边长全是三角数的勾股三角形，例如：

$$\left(\frac{132\times133}{2}\right)^2+\left(\frac{143\times144}{2}\right)^2=\left(\frac{164\times165}{2}\right)^2.$$

但由第九节可知，没有两条边是平方数的勾股三角形．有一条边是平方数的勾股三角形当然有无穷多个．

另一方面，我们却有下面的颇为有趣的结论．

例 6　对每个正整数 $n>1$，都有勾股三角形，使其每条边的长度都是不小于 n 次的方幂．

证明　我们的方法是构造性的．任取一组勾股数(a, b, c)，令

$$k=a^{4n^2-1}b^{2n(n-1)(2n+1)}c^{2n^2(2n-1)},$$

则勾股数 ak，bk，ck 都是 $\geqslant n$ 的方幂．

关于勾股三角形的面积与周长，也有一系列问题．

例 7　对每个正整数 $n>1$，都有一个本原的勾股三角形，其周长是 n 次方幂．

证明　我们仍采用构造性的方法．设 $t\geqslant n>1$，取

$$a=2^{n-1}t^n,\ b=(2t-1)^n-a,$$

则 b 必是正整数(这是一个不等式的练习，请读者自己证明)．

又明显 a 为偶数, b 是奇数.

设 p 为 a 的奇素因数, 则 $p|t$, 从而 $b\equiv(-1)^n(\bmod p)$, 于是 $p\nmid b$, 故 $(a, b)=1$.

边长为 a^2-b^2, $2ab$, a^2+b^2 的三角形是本原的勾股三角形. 它的周长

$$\begin{aligned}(a^2-b^2)+2ab+(a^2+b^2)\\=2a(a+b)=(2t(2t-1))^n\end{aligned}$$

是整数的 n 次方幂. 证毕.

如果不要求三角形是本原的, 问题很容易解决. 这只要将任意勾股三角形的各边乘上其周长的 $n-1$ 次幂就行了.

例 8　对于每个正整数 n, 存在 n 个(互不全等的)勾股三角形, 它们的周长相等.

证明　由定理得知, 存在无穷多个互不相似的勾股三角形. 我们从中任取 n 个, 设为

$$a_k,\ b_k,\ c_k(a_k<b_k<c_k,\ k=1,\ 2,\ \cdots,\ n).$$

令
$$a_k+b_k+c_k=s_k\quad(k=1,\ 2,\ \cdots,\ n).$$

取
$$s=s_1\times s_2\times\cdots\times s_n.$$

这样, 只要取

$$x_k=\frac{a_k s}{s_k},\quad y_k=\frac{b_k s}{s_k},\quad z_k=\frac{c_k s}{s_k},\qquad(k=1,\ 2,\ \cdots,\ n)$$

则 x_k, y_k, z_k 都是整数, 且对 $k=1, 2, \cdots, n$, 显然有

$$x_k^2+y_k^2=z_k^2$$

及
$$x_k+y_k+z_k=\frac{a_k}{s_k}s+\frac{b_k}{s_k}s+\frac{c_k}{s_k}s=s.$$

故勾股三角形 (x_k, y_k, z_k) 即为所求 $(k=1, 2, \cdots, n)$. 又因为我们取出的勾股三角形互不相似, 所以作出来的三角形互不全等, 证毕.

例 9 对每个正整数 n，都有 n 个勾股三角形（互不全等）面积相等.

证明 我们用归纳法来构造 n 个等积的勾股三角形，使它们斜边互不相同.

作为奠基，任取一个本原的勾股三角形，于是 $n=1$ 时，结论显然. 设对 n 结论成立，即假设 (a_k, b_k, c_k) $(k=1, 2, \cdots, n)$ 是斜边互不相等的、等积的勾股三角形，其中 c_1 是奇数.

令
$$a'_k=2c_1(b_1^2-a_1^2)a_k,$$
$$b'_k=2c_1(b_1^2-a_1^2)b_k,$$
$$c'_k=2c_1(b_1^2-a_1^2)c_k, \qquad (k=1, 2, \cdots, n)$$
$$a'_{n+1}=(a_1^2+b_1^2)^2-(2a_1b_1)^2,$$
$$b'_{n+1}=2\times 2a_1b_1(a_1^2+b_1^2),$$
$$c'_{n+1}=(2a_1b_1)^2+(a_1^2+b_1^2)^2.$$

显然 $$a_k'^2+b_k'^2=c_k'^2 \quad (k=1, 2, \cdots, n, n+1).$$

因为 $a'_{n+1}=(a_1^2-b_1^2)^2$，$b'_{n+1}=4a_1b_1c_1^2$，故这 $n+1$ 个勾股三角形 (a'_k, b'_k, c'_k) 的面积都等于 $2a_1b_1c_1^2(a_1^2-b_1^2)^2$.

此外，因 c_1 是奇数，故 $c'_{n+1}=(2a_1b_1)^2+c_1^4$ 是奇数，而 c'_k $(k=1, 2, \cdots, n)$ 都是偶数，所以 $c'_{n+1}\neq c'_k$ $(k=1, 2, \cdots, n)$. 至于 c'_k $(k=1, 2, \cdots, n)$ 互不相等则由归纳假设得知. 证毕.

注：由本例得知，如果已有 $n\geq 1$ 个面积都等于 d 的勾股三角形、斜边互不相等且至少有一个是奇数，则我们能由此构造出 $n+1$ 个面积都等于 ds^2 的勾股三角形、斜边互不相等且至少有一个为奇数. 这里 s 是一个正整数. 由此推出，存在任意多个互不全等的勾股三角形，它们的面积都等于给定的本原勾股三角形的面积乘以一个整数的平方. 这个注记在第十节例 12 中有用. 此外，在上面的构造中，我们是使三角形的斜边互不相等来保证它们互不全等的. 这个要求也是必要的，易于证明，如果两个直角三角形的面积和斜边对应相等，则它们全等.

由前面两个例子得知，我们能找到任意多个互不全等但

面积(或周长)相等的勾股三角形．然而周长等于面积(数值)的勾股三角形恰有两个，即(5, 12, 13)和(6, 8, 10)(见第三节例9)，其中只有一个是本原的．但是，边长为有理数的直角三角形中却有无穷多个面积(数值)和周长相等的．我们来确定这样的三角形．

例 **10**　求出所有边长为有理数，且面积(数值)等于周长的直角三角形．

解　对边长为有理数(将分母化为相同)$\frac{x}{t}<\frac{y}{t}<\frac{z}{t}$的直角三角形作相似比为$t$(即将边长扩大$t$倍)的相似变换，便得到边长为整数$x, y, z$的直角三角形；再作相似比为$\frac{1}{d}$的相似变换可使它变为本原的勾股三角形．这里$d=(x, y, z)$．

由定理，本原三角形的边长为

$$a^2-b^2,\ 2ab,\ a^2+b^2\ (a>b>0).$$

它的面积与周长的比

$$\frac{ab(a^2-b^2)}{(a^2-b^2)+2ab+(a^2+b^2)}=\frac{b(a-b)}{2}.$$

因此，原先的，面积与周长相等的直角三角形应由本原三角形按此比例缩小，即它的三边之长分别为

$$\frac{2(a+b)}{b},\ \frac{4a}{a-b},\ \frac{2(a^2+b^2)}{b(a-b)},\qquad ⑥$$

其中$a>b$为任意正整数．

本节的定理，可以用来解不定方程，这里举两个例子(其他的应用可参看后面两节)．

例 **11**　设A, B, C三点在一圆形池塘的边上，构成边长86米的正三角形(如图)．一个游泳者从A径直游向B，在游了x米后(到达E)，他转向正西方(也许，这时他遇到了一条蛇)，又游了y米到达池边D．如果$DE\parallel BC$，并且x,

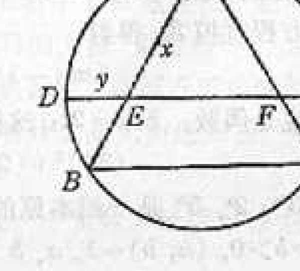
y 都是整数，试求出 y 的值.

解　延长 DE 分别交 AC 及圆周于 F, G 点. 易知

$$AE=AF=x,$$

且

$$FG=DE=y.$$



由圆幂定理，

$$AE\cdot BE=DE\cdot EG,$$

即

$$x(86-x)=y(x+y). \quad ⑦$$

⑦可化为

$$x^2+xy+y^2=86x. \quad ⑧$$

由⑧即知 x、y 都是偶数（否则 x^2+xy+y^2 是奇数）.

将⑧配方化成（这是关键性的一步）

$$\left(x+\frac{y}{2}-43\right)^2+y^2=\left(43-\frac{y}{2}\right)^2,$$

这表明 $\left|x+\frac{y}{2}-43\right|$, y, $43-\frac{y}{2}$ 是一组勾股数. 由定理的推论④可知，存在正整数 a, b, d, 使得

$$y=2abd,\ 43-\frac{y}{2}=(a^2+b^2)d.$$

从这两个式子可得

$$(a^2+ab+b^2)d=43. \quad ⑨$$

因 43 是素数，故 $d=1$,

$$a^2+ab+b^2=43. \quad ⑩$$

不难用估计与尝试得出⑩的正整数解为 $(a, b)=(6, 1)$ 或 $(1, 6)$. 从而 $y=12$, $x=2$ 或者 72.

例 12　证明不定方程

$$3^x+4^y=5^z \quad ⑪$$

的全部正整数解是 $x=y=z=2$.

证明　我们先来证明 x 及 z 都是偶数.

方程⑪模 4, 得到

$$(-1)^x \equiv 1 \pmod 4,$$

从而 x 是偶数. 设 $x=2x_1$,

方程⑪模 3, 得到

$$1 \equiv (-1)^z \pmod 3,$$

即 z 也是偶数. 设 $z=2z_1$, 这样⑪成为

$$(3^{x_1})^2+(2^y)^2=(5^{z_1})^2,$$

于是 3^{x_1}, 2^y, 5^{z_1} 是一组本原的勾股数. 由定理可知, 存在整数 $a>b>0$, $(a, b)=1$, a、b 一奇一偶, 使得

$$2^y=2ab, \qquad ⑫$$

$$3^{x_1}=a^2-b^2. \qquad ⑬$$

由⑫立即推出 $a=2^{y-1}$, $b=1$, 代入⑬, 得

$$3^{x_1}+1=2^{2(y-1)}. \qquad ⑭$$

如果 $y>2$, 则⑭的右边模 8 为 0. 但当 x_1 为偶数时, 3^{x_1} 是奇数的平方, 模 8 为 1; 当 x_1 为奇数时, $3^{x_1}=3\times3^{x_1-1}$, 模 8 为 3. 从而

$$3^{x_1}+1 \equiv 2, 4 \pmod 8,$$

矛盾. 因此必有 $y=2$, 这样 $x_1=1$, 即 $x=2$, $z=2$.

在不定方程中, 有一个涉及勾股数的著名猜想:

猜想　对于正整数 a, b, c 及 x, y, z, 如果

$$a^2+b^2=c^2, \quad a^x+b^y=c^z,$$

则

$$x=y=z=2.$$

例 12 表明, 在 $a=3$, $b=4$, $c=5$ 时猜想是正确的. 已经有人证明上述猜想对无穷多组勾股数成立, 但问题还远远没有完全解决.

九、无穷递降法

无穷递降法，是和费尔马的名字紧密地连在一起的，因此，本节的标题或许改为"费尔马的方法"更为确切．无穷递降法并不是一种神秘的方法．实际上，在第五节中我们已经用过这一方法．为了进一步说明什么是无穷递降法，先看一个简单的例子．

例1 设 $p\equiv-1\pmod 4$ 是一个素数，证明对任意正整数 n，方程

$$p^n=x^2+y^2 \qquad ①$$

没有正整数解 (x, y)．

证明 我们用反证法．假设对某个自然数 n，方程①有正整数解 (x_0, y_0)．不妨设 $(x_0, y_0)=1$．否则的话，设

$$(x_0, y_0)=d>1,$$

则由①知，$d^2|p^n$．因 p 是素数，所以 d 也是 p 的方幂．设

$$d=p^l \quad (1\leqslant 2l\leqslant n),$$

由①得
$$p^{n-2l}=\left(\frac{x_0}{d}\right)^2+\left(\frac{y_0}{d}\right)^2,$$

这样我们可以考虑代替①的方程

$$p^{n-2l}=x^2+y^2,$$

它有一组互素的正整数解 $\left(\frac{x_0}{d}, \frac{y_0}{d}\right)$．

x_0, y_0 显然一奇一偶，模4得

$$p^n\equiv(-1)^n\equiv x_0^2+y_0^2\equiv1 \pmod 4．$$

所以 n 是偶数．设 $n=2n_1 (n_1\geqslant1)$，则有

$$(p^{n_1})^2=x_0^2+y_0^2,$$

即(x_0, y_0, p^{n_1})是一组本原的勾股数(因为x_0和y_0互素). 由第八节的定理可知, 存在整数$a_1>b_1$, a_1, b_1一奇一偶, $(a_1, b_1)=1$. 使得

$$p^{n_1}=a_1^2+b_1^2.$$

同样的论证表明n_1必须是偶数, 并且设$n_1=2n_2$, $n_2\geqslant 1$(于是$n_1>n_2$). 则有正整数a_2, b_2, $(a_2, b_2)=1$, 使得

$$p^{n_2}=a_2^2+b_2^2.$$

反复进行下去, 便得到无穷多个正偶数$n_1>n_2>n_3>\cdots$, 这当然是不可能的.

上面的论证也可以改换成另一种形式:

设$n\geqslant 1$是使方程

$$p^n=x^2+y^2$$

有正整数解的n中最小的数. 如果(x_0, y_0)是一组解, 则与前面的解法一样, $(x_0, y_0)=1$(否则导出方程$p^{n-2l}=x^2+y^2$有正整数解$\left(\frac{x_0}{p^l}, \frac{y_0}{p^l}\right)$, 而$n-2l<n$, 这和$n$的选择矛盾), 并且$n$是偶数.

设$n=2n_1$, 由第八节的定理得知, 存在正整数$a, b, (a, b)=1$, 使得

$$p^{n_1}=a^2+b^2,$$

这意味着方程

$$p^{n_1}=x^2+y^2$$

有正整数解(a, b). 而

$$n_1=\frac{n}{2}<n,$$

和n的最小性矛盾.

不难看出，两种论证的实质是一样的，它们都依赖于一个基本的事实，即自然数的任一非空子集合中必有最小的数。采用哪种论证形式并不重要，读者可根据自己的喜好和习惯自由选择。

不定方程①也可以看作 x、y、n 的三元方程。这时例1的结论可以说成：方程①，在素数 $p\equiv -1 \pmod 4$ 时，无正整数解 (x, y, n)。上面的一种论证是解的无穷序列中，坐标 n 的值严格递减。另一种论证是在正整数解 (x, y, n) 中选一个坐标 n 最小的解，然后造出一个有更小 n 的解。

采用无穷递降法证明不定方程无正整数解（非平凡解、满足某些限制的解）的主要步骤是从相反的结论出发，假设存在一组正整数解，设法造出这个方程（或另一个同类的方程）的另一组正整数解，这新的解严格地比原来的解"小"。这里所说的"严格地小"，是指某一个与解有关的、取正整数值的量（函数）严格递减。这样的量可以取为解的某个坐标（或坐标的绝对值），如①的解 (x, y, n) 的第三坐标 n；或者坐标的和；或者其他有关的量，如 x、y 的二元方程①中的 p^n 的指数；等等。

如果上述过程可以无限地进行下去，那么由于严格递减的正整数数列只可能有有限多项（即必有最小数），两者产生矛盾。

论证的核心是设法造出新的（严格减少的）解。在处理有关平方数的问题时，第八节关于勾股数的定理是一个有力的工具，例1至例5均依靠它。在后面的几个例子中，一元二次方程的韦达定理大显神通。我们切不可忽视这一简单技巧的作用。

无穷递降法，并不只是用于否定方面。如果方程有解，那

么必有一组(或几组)最小的(正整数)解．采取递降法时，经过有限多步，必然到达最小解．因而递降法也给出了解的递推关系．

无穷递降法，不仅限于不定方程．许多问题，只要能从一种状态产生另一种状态，而且一个与状态有关的、取正整数值的量严格减少，就可以使用递降法．从这种意义上说，第一节的欧几里得算法其实就是一种无穷递降法(经过有限多步达到最小状态，即产生了最大公约数(a, b))．

下面的例2称为巴赫特(Bachet)问题，曾在第八节例5中提过．它是费尔马首先用无穷递降法予以证明的．这个问题与例3、例4有密切的关系．

例2 勾股三角形的面积不可能是完全平方数．

证明 用反证法．假设结论不对，我们在所有面积为平方数的勾股三角形中选取一个面积最小的(如果这样的三角形不止一个，则任取其中一个)，设它的三边分别为$x, y, z(x<y<z)$，$\frac{1}{2}xy$是平方数．我们的方法是使面积递降，即由此作出一个新的、面积也是平方数的勾股三角形，它的面积小于所取三角形的面积．这就导出矛盾．现在

$$x^2+y^2=z^2,$$

并且与例1相同，可以假定$(x, y)=1$$\Big($否则从方程可知$z$也被$(x, y)=d>1$整除，边长为$\frac{x}{d}$，$\frac{y}{d}$，$\frac{z}{d}$的三角形是勾股三角形，面积的4倍$2\cdot\frac{x}{d}\cdot\frac{y}{d}$是偶数，又是平方数，因而是4的倍数．从而面积$\frac{1}{2}\cdot\frac{x}{d}\cdot\frac{y}{d}$是平方数，小于$\frac{1}{2}xy$，矛盾$\Big)$．因此，由第八节定理可知，存在整数$a>b>0$，$a, b$一奇一偶，

$(a, b)=1$，使得（不妨设 y 为偶数）

$$x=a^2-b^2,\ y=2ab,\ z=a^2+b^2.$$

由于
$$\frac{1}{2}xy=(a-b)(a+b)ab$$

是完全平方数，而从 $(a, b)=1$ 及 $a-b$，$a+b$ 都是奇数，不难证明 $a-b$，$a+b$，a，b 这四个数两两互素，故它们都是平方数．即有整数 u，v，p，q 使

$$a=p^2,\ b=q^2,\ a+b=u^2,\ a-b=v^2. \tag{②}$$

所以
$$u^2-v^2=2q^2,$$

即
$$(u-v)(u+v)=2q^2. \tag{③}$$

注意 u，v 都是奇数，故
$$(u-v,\ u+v)=2.$$

从③式可知，$u-v$ 和 $u+v$ 中有一个是 $2r^2$，另一个是 $(2s)^2$，r，s 都是整数，$q^2=4r^2s^2$．另一方面，由②有

$$\begin{aligned}p^2=a&=\frac{1}{2}[(a+b)+(a-b)]\\&=\frac{1}{2}(u^2+v^2)=\frac{1}{4}[(u+v)^2+(u-v)^2]\\&=\frac{1}{4}[(2r^2)^2+(2s)^4]=r^4+4s^4.\end{aligned}$$

所以，以 r^2，$2s^2$，p 为边的三角形是勾股三角形，其面积等于

$$\frac{1}{2}r^2\times 2s^2=(rs)^2,$$

为平方数．而由②，③有

$$(rs)^2=\frac{q^2}{4}=\frac{b}{4}<(a^2-b^2)ab=\frac{1}{2}xy.$$

矛盾．

例 2 实际上是用无穷递降法证明了方程组

$$\begin{cases} x^2+y^2=z^2, \\ \frac{1}{2}xy=t^2 \end{cases}$$

无正整数解(x, y, z, t)（面积递降即坐标t递降）.

例 3 证明不定方程

$$x^4-y^4=z^2 \quad ④$$

没有y、z均不为 0 的整数解.

证明 如果④有整数解(x, y, z)，其中y、z均不为 0，则

$$x^4>x^4-y^4=z^2>0.$$

令
$$u=x^4-y^4,\ v=2x^2y^2,\ w=x^4+y^4,$$

则u、v、w都是正整数，而且u、v、w可以作为一个直角三角形的三条边. 这个三角形的面积为

$$\frac{1}{2}uv=x^2y^2(x^4-y^4)=x^2y^2z^2,$$

是完全平方数，与例 2 矛盾.

从例 3 可以导出下面的例 4.

例 4 证明不存在两个正整数，它们的平方和与平方差都是平方数.

证明 问题等价于方程组

$$\begin{cases} x^2+y^2=z^2, \\ x^2-y^2=t^2 \end{cases} \quad ⑤$$

没有正整数解.

将⑤的两个方程相乘便得

$$x^4-y^4=(zt)^2,$$

由例 3，此方程没有正整数解. 因此方程组⑤也没有正整数解.

例 3、例 4 都可以直接用无穷递降法证明. 例 4 可以推出例 3，例 3 也可以推出例 2. 这些均留给读者练习（习题 35

及36).

研究不定方程是费尔马的一大嗜好．他所考虑的问题在很大程度上刺激了现代数论的发展，特别是著名的费尔马大定理．

费尔马大定理　对于正整数 $n\geqslant 3$，方程

$$x^n+y^n=z^n \tag{⑥}$$

没有非平凡(即 $xyz\neq 0$)的整数解 (x, y, z)．

几百年来，众多的数学家(专业或业余的)企图证明这个"大定理"，一直没有成功．所以费尔马大定理实际上仍是一个大猜想．

最近，伐尔廷斯(Faltings)证明了一个更一般的猜想，从而推出，对每个 $n\geqslant 4$，方程⑥至多有有限组非平凡的整数解．在这里，将解 (x, y, z) 和 (dx, dy, dz) 看作是同一组解，d 是任意整数．

我们提醒一件有趣的事．由第六节例7可知，方程

$$x^n+y^n=z^{n+1}$$

和

$$x^n+y^n=z^{n-1}$$

都有无穷多组正整数解 (x, y, z)．这里 $n\geqslant 2$．这两个方程与⑥相比只是 z 的方幂增减一个"1"．可谓"失之毫厘，差之千里"．

要证明费尔马大定理，只要对 $n=4$ 以及 n 为奇素数来证明就够了．因为如果这些已被证实，则对任意 $n>2$，在有奇素数 $p|n$ 时，由方程

$$x^p+y^p=z^p$$

无非平凡解推出方程

$$(x^{\frac{n}{p}})^p+(y^{\frac{n}{p}})^p=(z^{\frac{n}{p}})^p,$$

也就是方程⑥无非平凡解．

如果 n 没有奇素因子，则 n 是 2 的方幂. 因 $n>2$，故 $4|n$. 同上面一样可表明此时⑥也无非平凡解.

对于奇素数 $n=p<125000$ 的情况，费尔马大定理已经证明，论证都是非常困难的. 但对于 $n=4$，我们可以采用无穷递降法，这种情况的证明是费尔马本人完成的. 实际上，他证明了略强的结论:

例 5 方程

$$x^4+y^4=z^2 \qquad ⑦$$

没有非平凡的整数解 (x, y, z).

(例 5 显然能推出方程

$$x^4+y^4=(z^2)^2$$

没有非平凡的整数解).

证明 假设⑦有一组整数解 $xy\neq 0$，可设 $x>0$, $y>0$, $z>0$. 我们在所有这样的解中选取一组使 z 最小的解. 如果这样的解不止一组，则任取一组. 论证的想法是(类似于例 2 的解法)造出另一组正整数解 (r, s, t)，使得 $0<t<z$. 由于 z 已选择为最小，这就导出矛盾.

先请注意，此时必有 $(x, y)=1$. 否则就有素数 $p|(x, y)$. 从而 $p^4|z^2$，即 $p^2|z$，所以

$$\left(\frac{x}{p}\right)^4+\left(\frac{y}{p}\right)^4=\left(\frac{z}{p^2}\right)^2.$$

这就得出⑦的一组新的非平凡解 $\left(\frac{x}{p}, \frac{y}{p}, \frac{z}{p^2}\right)$，但 $\frac{z}{p^2}<z$，和 z 的选择矛盾.

将⑦改写成为

$$(x^2)^2+(y^2)^2=z^2,$$

由于 $(x, y)=1$，故 $(x^2, y^2)=1$. 于是 (x^2, y^2, z) 成为一组本原

的勾股数. 由第八节的定理可知, 存在整数 $a>b>0$, $(a, b)=1$, a, b 一奇一偶, 使得(不妨设 y 为偶数)

$$x^2=a^2-b^2,\ y^2=2ab,\ z=a^2+b^2. \qquad ⑧$$

由

$$x^2+b^2=a^2$$

以及 $(a, b)=1$ 可知 a 是奇数, b 是偶数, 再应用第八节的定理知, 存在整数 $p>q>0$, $(p, q)=1$, p, q 一奇一偶, 使

$$x=p^2-q^2,\ b=2pq,\ a=p^2+q^2,$$

代入⑧得到

$$y^2=4pq(p^2+q^2),$$

即

$$\left(\frac{y}{2}\right)^2=pq(p^2+q^2).$$

因 $(p, q)=1$, 易知 p, q, p^2+q^2 两两互素. 由上式知它们都是平方数, 即有正整数 r, s, t 使

$$p=r^2,\ q=s^2,\ p^2+q^2=t^2,$$

从而

$$r^4+s^4=t^2.$$

于是我们得出了⑦的一组非平凡解 (r, s, t). 但是

$$0<t=\sqrt{p^2+q^2}=\sqrt{a}<\sqrt[4]{z}<z.$$

和 z 的最小性矛盾.

由本例立即推出, 勾股三角形的两条直角边不可能都是完全平方数. 因而勾股三角形的面积也不可能是平方数的两倍.

例 1 至例 5 是费尔马本人处理过的经典问题, 均与勾股三角形密切相关. 下面将用无穷递降法讨论另一种类型的不定方程. 先看一道国际数学竞赛题.

例 6 设正整数 a, b 使得 $ab+1\mid a^2+b^2$, 证明 $\dfrac{a^2+b^2}{ab+1}$ 是完全平方数.

证法一　设 $\frac{a^2+b^2}{ab+1}=q$（q 是正整数），则

$$a^2+b^2=q(ab+1). \tag{9}$$

将⑨看成 a、b 的二元方程．显然 $a=b$ 将导出 $q=1$．我们设 $a>b$，并且在这种解中，第一坐标最小的是 (a_0, b_0)．

考虑 x 的一元二次方程

$$x^2-qb_0x+b_0^2-q=0. \tag{10}$$

它已有解 $x=a_0$．根据韦达定理，另一解为 $a_1=qb_0-a_0$．也是整数，而且非负，否则

$$a_1^2-qb_0a_1+b_0^2-q>-qb_0a_1-q\geqslant q-q=0.$$

$a_1=0$ 将导出 $q=b_0^2$．如果 q 不是完全平方，则 a_1 为正整数．这时 (b_0, a_1) 是⑨的正整数解，并且

$$a_1=\frac{b_0^2-q}{a_0}<\frac{b_0^2-1}{b_0}<b_0.$$

这与假设 (a_0, b_0) 的第一坐标 a_0 为最小矛盾．从而 q 是完全平方数．

证法二　设 $\frac{a^2+b^2}{ab+1}=q$，若 $q=1$，则 $a=b=1$．若 $q=2$，则 $(a-b)^2=2$，无解．下面考虑 $q\geqslant3$，并有

$$a^2+b^2=q(ab+1). \tag{11}$$

不妨设 $a>b$（证法一中已说过 $q>1$ 时 $a\neq b$），因为

$$a^2=qab+q-b^2>qab-ab=(q-1)ab,$$

所以
$$a>(q-1)b.$$

另一方面，若 $a>qb$，则有

$$q=a(a-qb)+b^2\geqslant a+b^2>qb\geqslant q.$$

矛盾．因此
$$(q-1)b<a\leqslant qb.$$

设（相当于带余除法）

$$a=qb-r\quad(0\leqslant r<b),$$

代入⑪得 $$(qb-r)^2+b^2=q((qb-r)b+1),$$

即

$$b^2+r^2=q(br+1). \tag{12}$$

由此可见数对(b, r)取代了⑪中的(a, b). 一般地,若

$$a_n^2+b_n^2=q(a_nb_n+1) \quad (a_n\geqslant b_n>0,\ n\geqslant 1),$$

则(类似于欧氏算法)

$$a_n=qb_n-r_n \quad (0\leqslant r_n<b_n), \tag{13}$$

并且在$r_n\neq 0$时,有

$$a_{n+1}^2+b_{n+1}^2=q(a_{n+1}b_{n+1}+1), \tag{14}$$

其中

$$a_{n+1}=b_n,\ b_{n+1}=r_n. \tag{15}$$

令$a_1=a$, $b_1=b$, $r_1=r$. 由⑬, ⑮得到两个正整数数列$\{a_n\}$, $\{b_n\}$, 且$\{a_n\}$严格递降,因而它仅有有限多项,即存在l,使得$r_l=0$. 这时$a_l=qb_l$, 而$q=b_l^2$. 证毕.

满足$ab+1|a^2+b^2$的a, b显然有无穷多对,例如$a=b^3$即是. 我们能够求出全部的解.

例 7 求出$ab+1|a^2+b^2$的全部正整数解(a, b).

解 显然$(a, b)=(1, 1)$是解. 若

$$\frac{a^2+b^2}{ab+1}=q\geqslant 3.$$

在上面的证法二中,改记$b_l=k$, 则$q=k^2$($k\geqslant 2$为整数). 又改记

$$a_1,\ a_2,\ \cdots,\ a_l;\ b_1,\ b_2,\ \cdots,\ b_l$$

为 $$A_l,\ A_{l-1},\ \cdots,\ A_1;\ B_l,\ B_{l-1},\ \cdots,\ B_1.$$

则⑬, ⑮即为

$$A_{m+1}=qA_m-A_{m-1} \quad (1\leqslant m\leqslant l-1), \tag{16}$$

其中 $$A_0=B_1=b_l=k,\ A_1=a_l=qk=k^3.$$

由上面的递推公式及初值 A_0, A_1, 不难求出

$$a=A_l=\frac{k}{\sqrt{k^4-4}}\left[\left(\frac{k^2+\sqrt{k^4-4}}{2}\right)^{l+1}-\left(\frac{k^2-\sqrt{k^4-4}}{2}\right)^{l+1}\right],$$

$$b=B_l=\frac{k}{\sqrt{k^4-4}}\left[\left(\frac{k^2+\sqrt{k^4-4}}{2}\right)^{l}-\left(\frac{k^2-\sqrt{k^4-4}}{2}\right)^{l}\right]$$

$(l=1, 2, \cdots, k\geqslant 2)$.

这就是所求的全部正整数解(a, b).

证法一中的 $a_1=qb_0-a_0$ 其实就是递推公式⑯.

例 8 证明如果方程

$$x^2+y^2+1=xyz \tag{17}$$

有正整数解(x, y, z), 则必有 $z=3$.

证明 用反证法. 假设有正整数 $z\neq 3$ 使方程⑰有正整数解(x, y), 则 $x\neq y$. 否则得出

$$2x^2+1=x^2z,$$

即
$$x^2(z-2)=1,$$

推出 $x=1$ 和 $z=3$. 矛盾.

由于 x 与 y 是对称的, 不妨设 $x>y$. 在这种解中取第一坐标最小的, 设为(x_0, y_0). 与例 6 类似, 考虑 x 的一元二次方程

$$x^2-y_0zx+y_0^2+1=0. \tag{18}$$

由韦达定理, ⑱的另一个根为

$$x_1=y_0z-x_0,$$

这根是整数, 而且

$$0<x_1=\frac{y_0^2+1}{x_0}\leqslant\frac{y_0^2+1}{y_0+1}\leqslant y_0.$$

于是⑰又有一组正整数解(y_0, x_1), 满足 $y_0>x_1$(根据上面所说, $y_0\neq x_1$)及 $y_0<x_0$. 这与 x_0 的最小性矛盾.

在 $z=3$ 时，⑰有正整数解，而且有无穷多组．求法与例7类似．请看下例．

例 9　求出不定方程

$$x^2+y^2+1=3xy$$

的全部正整数解 (x, y)．

解　由于对称性，不妨只考虑 $x\geqslant y$ 的解 (x, y)．当 $x=y$ 时，方程只有一组解 $x=y=1$．以下考虑 $x>y$ 的情形．

例8中的 $x_1=y_0z-x_0$ 现在成为

$$x_1=3y_0-x_0. \qquad ⑲$$

它可以作为从一组解 (x_0, y_0) 到另一组解 (y_0, x_1) 的递推公式．这个递推过程可以继续下去，直至两个坐标相等，即 (x_0, y_0) 是 $(1,1)$（有趣的是，如果再使用⑱，则逐一产生出与前面相同的解，只不过两个坐标恰好交换．即

$$\cdots\to(233, 89)\to(89, 34)\to(34, 13)\to(13, 5)$$
$$\to(5, 2)\to(2, 1)\to(1, 1)\to(1, 2)\to(2, 5)$$
$$\to(5, 13)\to(13, 34)\to(34, 89)\to(89, 233)\to\cdots.$$

将⑲改写成

$$x_0=3y_0-x_1,$$

然后自 $(1, 1)$ 起，依逆推顺序重新编号，则上式就是解 (u_n, u_{n-1}) 的递推公式

$$u_{n+1}=3u_n-u_{n-1}. \qquad ⑳$$

用这个公式不难算出上面列出的那些解．

我们不难看出，在上面的解答中，实现递降的第一步，即 $x_1=3y_0-x_0$ 相当于带余除法，而整个递降过程则类似于欧氏算法．当递降停止后，我们倒回去求得了任一组解．这种方法类似于第一节中使用过的方法．在那里，我们从求 (a, b) 的欧氏算法倒推回去，求出了方程

$$ax+by=(a, b)$$
的一组整数解 x, y.

形如 $$x^2+y^2+z^2=3xyz$$
的方程称为马尔可夫(Markoff)方程(取 $z=1$ 便是例 9 中考虑过的方程). 马尔可夫方程有无穷多组正整数解.

例 10 求出不定方程
$$x^2+y^2+z^2=3xyz \tag{21}$$
的全部正整数解 (x, y, z).

解 由 x, y, z 的对称性, 我们只需求出满足 $x\geqslant y\geqslant z>0$ 的正整数解 (x, y, z).

首先我们考虑 x, y, z 中至少有两个相等的情形. 如果 $x=y=z$, 则显然 $x=y=z=1$; 如果 $x=y>z$, 则有
$$2x^2+z^2=3x^2z,$$
所以 $x^2|z^2$ 即 $z\geqslant x$. 矛盾. 此时无解.

假如 $x>y=z$, 则有
$$x^2+2y^2=3xy^2,$$
显然 $y^2|x^2$ 即 $y|x$. 设 $x=ay$, $a>0$, 则得
$$2+a^2=3ax,$$
所以 $a|2$, 故 $a=1$ 或者 2. 但 $x>y$ 故 $a\neq1$. 若 $a=2$ 便有 $y=z=1$ 以及 $x=2$, 而得解 $(2, 1, 1)$.

下面考虑满足 $x>y>z$ 的正整数解 (x, y, z). x 是一元二次方程
$$f(t)=t^2-3tyz+y^2+z^2=0$$
的一个根. 设其另一个根为 x', 则
$$x'+x=3yz,\quad xx'=y^2+z^2,$$
于是 $x'=3yz-x$ 也是正整数. 此外
$$(y-x)(y-x')=f(y)=2y^2-3y^2z+z^2$$

$$=(2-2z)y^2+(z^2-zy^2)<0.$$

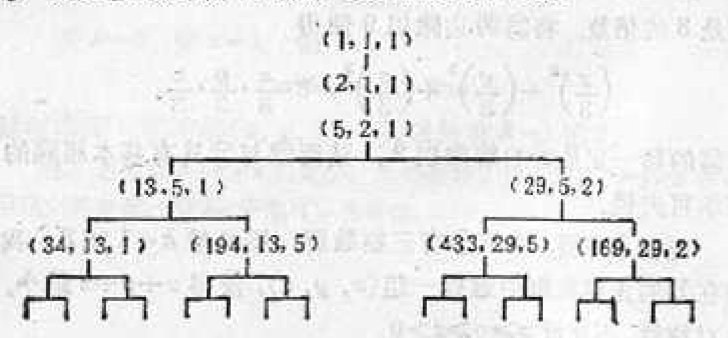
由于 $y<x$，所以 $y>x'$（x' 与 z 的大小不能确定是无关紧要的）.

这样，我们得到一组新的解 (y, x', z)，其中最大的坐标 y 小于解 (x, y, z) 中最大的坐标 x.

如果 $x'\neq z$，则又可以按照上面的方法造出新解．这样继续下去，经过有限多步必然出现后面两个坐标相同的情况，即达到解 $(2, 1, 1)$.

反过来，由 $(2, 1, 1)$ 可以推出㉑的所有解．但在将上述过程逆回去的时候，需要注意有两种可能．即 (y, x', z) 可以逆推出解 $(3yz-x', y, z)$ 或 $(3yx'-z, y, x')$.

下图显示了逆推的结果，它称为解的"马尔可夫链"．[$(2, 1, 1)$ 也可以看成由 $(1, 1, 1)$ 逆推而得，因为 $2=3\times1\times1-1$] 每一组正整数解或早或迟，都必然在链中出现.



最后我们考虑一般形式的方程

$$x^2+y^2+z^2=kxyz, \tag{㉒}$$

这里 k 是一个正整数．$k=3$ 时方程即㉑．在第五节例 17 中，证明了 k 为偶数时，㉒仅有平凡解 $(0, 0, 0)$.

例 11　当且仅当 $k=1$ 或 3 时，方程㉒有非平凡的整

数解.

证明 如果x、y、z中有一个为0，则由㉒，其他两个也必然为0. 如果x、y、z中有负的，则用它的相反数来代替，这时解就成为非负的. 因此，我们只需证明

当且仅当$k=1$或3时，方程㉒有正整数解.

充分性是明显的. $k=3$的情况即例10. $k=1$时，方程有解(3, 3, 3). 不仅如此，将方程

$$x^2+y^2+z^2=3xyz \tag{㉑}$$

两边乘以9得

$$(3x)^2+(3y)^2+(3z)^2=(3x)(3y)(3z)$$

所以㉑的每一组解(的各个坐标)乘以3便得出

$$x^2+y^2+z^2=xyz \tag{㉓}$$

的一组解.

反过来，用第五节的方法(模3)易知㉓的解的每一坐标都是3的倍数. 将㉓两边除以9便得

$$\left(\frac{x}{3}\right)^2+\left(\frac{y}{3}\right)^2+\left(\frac{z}{3}\right)^2=3\cdot\frac{x}{3}\cdot\frac{y}{3}\cdot\frac{z}{3}.$$

即㉓的解一定是㉑的解乘以3. 从而㉓与㉑具有基本相同的马尔可夫链.

现在来证明，如果㉒有正整数解，则必然$k=1$或3. 我们在㉒的正整数解中选择一组(x, y, z)，使得$x+y+z$最小，由对称性，不妨设$x\geqslant y\geqslant z>0$.

令
$$x'=kyz-x,$$

则与例10同样可证(x', y, z)也是㉒的一组正整数解. 这样就有$x'+y+z\geqslant x+y+z$. 从而

$$x'=kyz-x\geqslant x, \tag{㉔}$$

由㉔得到

$$x<\frac{1}{2}kyz,$$ ㉕

又显然有 $\qquad 3x^2-kxyz=2x^2-y^2-z^2\geqslant 0,$

即

$$x\geqslant\frac{1}{3}kyz.$$ ㉖

将方程㉒变形为

$$y^2+z^2+\left(x-\frac{1}{2}kyz\right)^2-\left(\frac{1}{2}kyz\right)^2=0.$$

利用㉕，㉖得出

$$y^2+z^2+\frac{1}{36}k^2y^2z^2-\frac{1}{4}k^2y^2z^2\geqslant 0,$$

因 $y\geqslant z$，故有

$$2y^2\left(1-\frac{k^2z^2}{9}\right)\geqslant 0,$$

于是 $\qquad k^2z^2\leqslant 9,$

即 $\qquad kz\leqslant 3.$

若 $k=2$，则 $z=1$．但

$$x^2+y^2+1>2xy,$$

这时㉒不可能有解$(x,\ y,\ 1)$．所以只有 $k=1$ 或 3．

注：选择最 $x+y+z$ 为最小，无非是为了免去讨论 $x\geqslant y\geqslant z$ 中等号成立的情况．例 10 中也可以这样做．

十、杂　例

本节讨论一些特殊的问题，可以看作是前几节的补充和应用，其中包括一些四次方程及两个古老问题的最新结果。

在第八节中，我们指出方程

$$x^2+y^2=z^2 \qquad ①$$

有无穷多组正整数解（并求出了全部本原解）。这个结果可以表达为：有无穷多对正整数的平方和是完全平方数。由此我们可以稍稍走远一点。

例1　存在正整数的无穷数列 $\{a_n\}$，使得对任意 $n>1$，$a_1^2+a_2^2+\cdots+a_n^2$ 都是完全平方数。

证明　用归纳法来构造这样的数列。论证的出发点是恒等式（即方程①的一组解）：

$$(2k-1)^2+(2k^2-2k)^2=(2k^2+2k+1)^2.$$

先取正整数 a_1，a_2（$a_1<a_2$），使 $a_1^2+a_2^2$ 是奇数的平方。这只要取①的一组本原解就够了。

假设已作出了 $a_1<a_2<\cdots<a_n$，使得 $a_1^2+a_2^2+\cdots+a_n^2$ 是奇数的平方，设为 $(2k+1)^2$。现在取 $a_{n+1}=2k^2+2k$，则（由上述恒等式）

$$a_1^2+a_2^2+\cdots+a_n^2+a_{n+1}^2=(2k^2+2k+1)^2,$$

也是奇数的平方。由此便（递推地）作出了符合要求的无穷数列。

与方程①有关的另一个问题是：能否找出三个正整数，使得它们两两平方之和都是完全平方数？这是第六节中例10的

加强命题．回答是肯定的，我们可以用方程①的解来证明．

例 2　有无穷多个正整数的三数组(a, b, c)，使得

$$a^2+b^2,\ a^2+c^2,\ b^2+c^2$$

都是完全平方．

证明　还是采用构造法．任取①的一组正整数解(x, y, z)（不必本原）．设

$$a=x\left|4y^2-z^2\right|,\ b=y\left|4x^2-z^2\right|,\ c=4xyz,$$

则有
$$a^2+b^2=(z^3)^2,\ a^2+c^2=x^2(4y^2+z^2)^2,$$

$$b^2+c^2=y^2(4x^2+z^2)^2.$$

由于①有无穷多组解，这样就证得了符合要求的三数组有无穷多个．

特别地，取$x=3$，$y=4$，$z=5$，得出$a=117$，$b=44$，$c=240$，并且

$$117^2+44^2=125^2,\ 117^2+240^2=267^2,\ 44^2+240^2=241^2.$$

例 2 的几何意义是显然的，即存在无穷多个棱长都是整数且有三条自同一顶点引出的棱两两垂直的四面体．但是目前还不知道是否有一个长方体，它的三度、各个面的以及自身的对角线长都是整数．即不知是否有正整数x, y, z，使得x^2+y^2，y^2+z^2，z^2+x^2，$x^2+y^2+z^2$都是完全平方数．

等差数列一直是数论中感兴趣的课题．1^2，5^2，7^2；7^2，13^2，17^2；……都是成等差数列的平方数．一般地，设整数$0<x<y<z$，且x^2，y^2，z^2成等差数列，则

$$x^2+z^2=2y^2. \qquad ②$$

因此，求出所有成等差数列的平方数三数组就等价于确定②的全部正整数解(x, y, z)，$0<x<y<z$（我们不考虑公差为 0 这种平凡的情形）．

例 3　证明方程②满足$0<x<y<z$的全部正整数解为

$$x=|a^2-b^2-2ab|d,\ y=(a^2+b^2)d,\ z=(a^2-b^2+2ab)d. \quad ③$$

这里 $a>b>0$, a, b 一奇一偶, $(a, b)=1$, d 是任意正整数.

证明　不难验证, 如果 a, b, d 满足上面说的要求, 则由③确定的 (x, y, z) 是②的满足 $0<x<y<z$ 的解.

反过来, 我们先考虑②的满足 $(x, z)=1$ 的解. 这时 y 不能是偶数, 否则对②取模 4 即知 $x\equiv z\equiv 0 \pmod 2$, 和 $(x, z)=1$ 矛盾. 所以 y 是奇数, 从而 x, z 都是奇数, $z+x$, $z-x$ 都是偶数. 设

$$z+x=2u,\ z-x=2v.$$

u, v 都是正整数. 即 $x=u-v$, $z=u+v$. 代入②得

$$u^2+v^2=y^2.$$

显然 $(u, v)=1$, 故由第八节中的定理可知, 存在整数 $a>b>0$, $(a, b)=1$, a, b 一奇一偶, 使得

$$u=a^2-b^2,\ v=2ab,\ y=a^2+b^2,$$

或者 $$u=2ab,\ v=a^2-b^2,\ y=a^2+b^2.$$

但无论哪种情况都有

$$x=u-v=|a^2-b^2-2ab|,$$

$$z=u+v=a^2-b^2+2ab.$$

这就证明了当 $(x, z)=1$ 时的结论(在③中取 $d=1$).

当 $(x, z)\neq 1$ 时, 设 $(x, z)=d$. 从②知 $d^2|2y^2$. 若 $2\nmid d$, 显然有 $d|y$; 若 $2|d$, 也不难证明 $d|y$(请读者自己完成). 总之 $d|y$. 将方程②化为

$$\left(\frac{x}{d}\right)^2+\left(\frac{z}{d}\right)^2=2\cdot\left(\frac{y}{d}\right)^2, \quad ④$$

这时 $$\left(\frac{x}{d}, \frac{z}{d}\right)=1,$$

对④应用前面得到的结果可知，存在整数 $a>b>0$，$(a,b)=1$，a，b 一奇一偶，使

$$\frac{x}{d}=|a^2-b^2-2ab|,\ \frac{y}{d}=a^2+b^2,\ \frac{z}{d}=a^2-b^2+2ab,$$

这正是③的形式．证毕．

我们求出了所有成等差数列（公差不为0）的平方数的三数组．但请注意，数列的公差不可能是（非零）平方数．因为如果有整数 $t\neq0$，使得

$$\begin{cases}y^2-x^2=t^2,\\ z^2-y^2=t^2,\end{cases}$$

就有

$$\begin{cases}y^2-t^2=x^2,\\ y^2+t^2=z^2.\end{cases}$$

因 $t\neq0$，这和第九节例4的结果相违．

或许有读者希望找到由平方数组成的四项等差数列，但实际上是不可能的，除非四个数相等，即公差为0．费尔马在三百多年前就看出了这一点，我们在例10中给予证明．

此外，不难证明，存在无穷多个、由互不相等的三角数组成的三项等差数列．因为

$$\frac{x(x+1)}{2}+\frac{z(z+1)}{2}=2\cdot\frac{y(y+1)}{2}$$

等价于 $$(2x+1)^2+(2z+1)^2=2(2y+1)^2,$$

我们只要找到三个成等差的奇数的平方就够了．由例3这显然有无穷多组．

然而没有互不相等的三个立方数能组成等差数列．这结论的证明较为困难，本书不予讨论．也没有三个互不相等的四次方幂组成等差数列．请见后面的例7．

前面我们用到了第九节中的例4，即没有两个正整数的

平方和及平方差都是完全平方．然而却有无穷多对三角数，它们的和及差都是三角数．现在我们来证明它．

例 4　有无穷多对三角数，它们的和及差都是三角数．

证明　问题相当于要证明方程组

$$\begin{cases}\dfrac{x(x+1)}{2}+\dfrac{y(y+1)}{2}=\dfrac{z(z+1)}{2},\\[2mm]\dfrac{x(x+1)}{2}-\dfrac{y(y+1)}{2}=\dfrac{t(t+1)}{2}\end{cases}$$

有无穷多组正整数解 (x, y, z, t)．上式显然与

$$\begin{cases}(2x+1)^2+(2y+1)^2=(2z+1)^2+1, & ⑤\\ (2x+1)^2-(2y+1)^2=(2t+1)^2-1 & ⑥\end{cases}$$

同解．

将⑤，⑥相加，得到

$$(2z+1)^2+(2t+1)^2=2(2x+1)^2. \qquad ⑦$$

我们利用例 3 来选择⑦的无穷多组解为

$$\begin{aligned}&2t+1=\left|a^2-b^2-2ab\right|,\ 2x+1=a^2+b^2,\\ &2z+1=a^2-b^2+2ab.\end{aligned} \qquad ⑧$$

这里 a 为正偶数，b 为正奇数．具体的 a，b 将在下面选取．

将⑧代入⑤并化简，得到

$$(2y+1)^2=4ab(a^2-b^2)+1,$$

即

$$y(y+1)=ab(a^2-b^2).$$

现在尝试着(是尝试！而非必然)选取

$$ab=y+1,\ a^2-b^2=y, \qquad ⑨$$

即要求 a，b 满足

$$a^2-b^2-ab+1=0. \qquad ⑩$$

配方成为(a 为偶数，b 是奇数)

$$\left(b+\frac{a}{2}\right)^2-5\cdot\left(\frac{a}{2}\right)^2=1,$$

这就归结成一个佩尔方程

$$u^2-5v^2=1.$$

它有解 $u=9$, $v=4$, 故有无穷多组正整数解 (u, v), 显然 $u>v$, 并且 u 为奇数, v 为偶数. 因此, 我们可选取

$$a=2v,\ b=u-v,$$

这就得出满足⑩的无穷多组正整数 a, b. 且 $2|a$, $2\nmid b$. 对这样的 a, b, 从⑧, ⑨可知, 选取

$$2x+1=a^2+b^2,\ 2y+1=2ab-1,$$

$$2z+1=3ab-1,\ 2t+1=ab+1,$$

就得到方程组⑤, ⑥的无穷多组正整数解 (x, y, z, t). 证毕.

特别地, 取 $a=8$, $b=5$, 得到 $x=44$, $y=39$, $z=59$, $t=20$, 从而有

$$\frac{44\times45}{2}+\frac{39\times40}{2}=\frac{59\times60}{2},$$

$$\frac{44\times45}{2}-\frac{39\times40}{2}=\frac{20\times21}{2}.$$

上面的问题都与整数的平方和有关, 这方面有许多有趣的结果. 我们再举几个.

例 5 有无穷多个连续整数的三数组, 其中每一个都是两个正整数的平方和.

证明 取 $x=2n^4+4n^3+2n^2$,

则

$$x=(n^2+n)^2+(n^2+n)^2,$$

$$x+1=[n(n+2)]^2+(n^2-1)^2,$$

$$x+2=(n^2+n+1)^2+(n^2+n-1)^2.$$

其中 n 为大于 1 的整数. 这样 $(x, x+1, x+2)$ 便是符合要求

的三数组，当然有无穷多组.

不难看出，要求四项则又不可能，即不会有连续四个整数使得每一个都是两个正整数的平方和. 因为这样的四个数中必有一个模 4 同余于 3. 它甚至不可能表示成两个整数的平方和（模 4 即知）. 注意：能表示成两个整数的平方和并不意味着它也能表示成两个正整数的平方和. 例如，设素数 $p\equiv -1 \pmod 4$，则平方数 p^{2n}（有无穷多个！）当然是两个整数的平方和：$p^{2n}=0^2+(p^n)^2$. 但由第九节例 1 可知它不能是两个正整数的平方和.

例 6　有无穷多个完全平方数不能表示成三个正整数的平方和.

证明　1 不能表示成三个正整数的平方和. 采用第五节例 18 的证法即知 2^{2k}（k 是非负整数）不能表示成三个正整数的平方和，即方程

$$(2^k)^2=x^2+y^2+z^2 \tag{11}$$

没有正整数解 (x, y, z).

正整数这一限制至关重要，如果允许 x, y, z 取 0，则⑪显然有解.

同样可以证明 $(5\times 2^k)^2$（k 是非负整数）不能表示成三个正整数的平方和（习题 37）. 有趣的是，还能证明当且仅当 n 不具有 2^k, 5×2^k（k 为非负整数）形式时，n^2 能表示成三个正整数的平方和.

我们在第五节中曾经说过，每个正整数都可以表示成四个整数的平方和. 但它们未必可表示成四个正整数的平方和. 能够证明，当且仅当 n 不是 1, 3, 5, 9, 11, 17, 29, 41, 2×4^k, 6×4^k, 14×4^k（k 为非负整数）时，n 可以表示成四个正整数的平方和. 其必要性请看习题 38 题.

涉及到四次方幂的不定方程几乎都是很困难的。例如方程

$$\left(\frac{x(x+1)}{2}\right)^2=\frac{y(y+1)}{2},$$

有正整数解 $(x, y)=(1, 1), (3, 8)$. 即存在三角数，它的平方还是三角数. 但要证明仅有所说的两组解就很不容易. 以下我们考虑几个与前面内容有关的问题.

例 7 不可能有三个互不相等的四次方幂组成等差数列.

证明 实际上，我们能证明更强的结论，即方程

$$x^4+y^4=2z^2 \tag{12}$$

没有 $x\neq y$ 的整数解. 假如不然，不妨设 $x>y$. 又易知 x, y 的奇偶性相同，故

$$a=\frac{1}{2}(x^2+y^2),\ b=\frac{1}{2}(x^2-y^2),$$

都是正整数. 由⑫得到

$$\begin{cases} a^2+b^2=z^2, \\ a^2-b^2=(xy)^2, \end{cases}$$

因 $b\neq0$, 这和第九节例 4 矛盾.

也可以换一个方式来证，从⑫易知 $xyz\neq0$ 并且

$$(x^2+y^2)^4-(x^2-y^2)^4=(4xyz)^2,$$

因 $x^2-y^2\neq0$, 上式与第九节例 3 的结论矛盾.

例 8 证明大于 1 的三角数不会是四次方幂.

证明 假设结论不对，设

$$n(n+1)=2m^4\ (n>1).$$

如果 n 为偶数，设 $n=2k$, 则

$$k(2k+1)=m^4.$$

因 $(k, 2k+1)=1$, 于是 k 及 $2k+1$ 都是四次方幂，即有整数

x, y 使得

$$k=x^4,\ 2k+1=y^4,$$

所以

$$2x^4+1=y^4.$$

配方成为

$$(x^2)^4+y^4=(x^4+1)^2.$$

这和第九节例 5 的结论相违.

如果 n 是奇数, 设

$$n=2k+1(k\geqslant 1).$$

类似地存在整数 x, y, 使得

$$k+1=x^4,\ 2k+1=y^4,$$

于是

$$2x^4-1=y^4,$$

配方成为

$$(x^2)^4-y^4=(x^4-1)^2.$$

因 $k\geqslant 1$ 故 $x^4-1\neq 0$, 上式和第九节例 3 的结论矛盾. 证毕.

大于 1 的三角数也不会是三次方幂, 但本书不予证明.

例 9 证明不定方程

$$x^4-x^2y^2+y^4=z^2 \qquad ⑬$$

的正整数解由 $x=y, z=x^2$ 给出.

证明 采用无穷递降法. 假设方程有 $x\neq y$ 的正整数解. 我们在其中选择一组使 xy 最小的解. 与第九节例 5 一样地可证明, 此时必有 $(x, y)=1$. 由对称性不妨设 $x>y$, 将⑬配方成为

$$(x^2-y^2)^2+(xy)^2=z^2. \qquad ⑭$$

如果 x, y 一奇一偶, 可设 $y=2y_0$ 为偶数. 易知

$$(x^2-y^2,\ xy)=1,$$

由⑭及第八节的定理可知, 存在整数 $m>n>0$, m, n 一奇一偶, $(m, n)=1$, 使得

$$xy=2mn,\ x^2-y^2=m^2-n^2. \qquad ⑮$$

以 $y=2y_0$ 代入, 得到

$$y_0x=mn. \qquad ⑯$$

设 $(x, m)=a$, $(y_0, n)=b$. 将⑯化为

$$\frac{y_0}{b}\cdot\frac{x}{a}=\frac{m}{a}\cdot\frac{n}{b}.$$

由于
$$\left(\frac{x}{a}, \frac{m}{a}\right)=\left(\frac{y_0}{b}, \frac{n}{b}\right)=1,$$
故存在正整数 c, d 使得

$$\frac{x}{a}=\frac{n}{b}=c, \quad \frac{y_0}{b}=\frac{m}{a}=d,$$

即
$$x=ac, \ y_0=bd, \ m=ad, \ n=bc.$$
因 $(x, y_0)=1$, $(m, n)=1$. 故 a, b, c, d 两两互素. 将上式代入⑬中的 $x^2-y^2=m^2-n^2$, 得出

$$(a^2+b^2)c^2=(a^2+4b^2)d^2. \qquad ⑰$$

由于 $(a, b)=1$, 所以 $a^2+b^2\equiv 1$ 或 $2 \pmod 3$. 从而

$$(a^2+b^2, a^2+4b^2)=(a^2+b^2, 3b^2)=(a^2+b^2, b^2)$$
$$=(a^2, b^2)=1.$$

又 $(c, d)=1$, 由⑰及唯一分解定理可知

$$a^2+b^2=d^2, \ a^2+4b^2=c^2.$$

从 $a^2+4b^2=c^2$ 以及第八节的定理推出, 存在整数 $x_1>y_1>0$, 使得

$$a=x_1^2-y_1^2, \ 2b=2x_1y_1.$$

代入 $a^2+b^2=d^2$, 就有

$$x_1^4-x_1^2y_1^2+y_1^4=d^2,$$

这样, 我们就得到方程⑬的另一组正整数解 (x_1, y_1, d), $x_1\neq y_1$, 但是 $x_1y_1=b\leqslant n<2mn=xy$, 与 xy 的最小性矛盾.

如果 x, y 都是奇数, 由⑭知有整数 $m>n>0$, $(m, n)=1$, m, n 一奇一偶, 使得

$$x^2-y^2=2mn, \ xy=m^2-n^2,$$

从而 $$m^4-m^2n^2+n^4$$
$$=(m^2-n^2)^2+m^2n^2$$
$$=\left(\frac{x^2-y^2}{2}\right)^2+(xy)^2=\left(\frac{x^2+y^2}{2}\right)^2.$$
化成了上面讨论过的情况．

于是⑬的正整数解必须满足 $x=y$，从而 $z=x^2$．　证毕．

从例 9 就容易推出下述结论：

例 10　四个完全平方数不能组成公差不为 0 的等差数列．

证明　反证法．设有四个完全平方数 x^2, y^2, z^2, w^2($0<x<y<z<w$)，使得
$$x^2+z^2=2y^2,\ y^2+w^2=2z^2, \tag{18}$$
则有 $$x^2(2z^2-y^2)=w^2(2y^2-z^2),$$
即
$$2(x^2z^2-y^2w^2)=x^2y^2-w^2z^2. \tag{19}$$
将⑱模 4 可知 x, y, z, w 同奇同偶，故
$$c=\frac{1}{2}(xy+wz),\ d=\frac{1}{2}(xy-wz)$$
都是整数．

设 $xz=a$, $yw=b$．由⑲得出
$$a^2-b^2=2cd,\quad 及\quad ab=c^2-d^2,$$
从而 $$a^4-a^2b^2+b^4=(c^2+d^2)^2.$$
由上例得知，必须 $a=b$，即 $xz=yw$，
这和 $0<x<y<z<w$ 矛盾．证毕．

现在我们来看两个与费尔马大定理有关的四次方程．在第九节中已证明了方程
$$x^4+y^4=z^2$$

没有非平凡的整数解. 然而方程

$$x^4+y^4+z^4=t^2 \quad ⑳$$

(增加一个四次方幂)却有无穷多组正整数解, 这可利用勾股数来证明: 设正整数 a, b, c 满足

$$a^2+b^2=c^2,$$

则
$$(ab)^4+(ac)^4+(bc)^4=(c^4-a^2b^2)^2,$$

这就得出方程⑳的无穷多组正整数解.大数学家欧拉(Euler)在研究费尔马大定理时曾经考虑过方程⑳,他还猜想方程

$$x^4+y^4+z^4=t^4 \quad ㉑$$

没有 $xyz\neq 0$ 的整数解. 欧拉及后人都对方程㉑作过大量验证. 例如能够证明对于 $0<t<220000$, ㉑没有正整数解 (x, y, z). 这多少使人倾向于相信欧拉是对的. 然而, 最近埃尔基斯(Elkies)出人意料地否定了欧拉的猜想, 他借助于椭圆曲线的理论证明了方程㉑有无穷多组正整数解(由此又推出了⑳有无穷多组正整数解). 这里将 (x, y, z, t) 与 (dx, dy, dz, dt) 看作一样的解, d 为任意整数.

另一方面,欧拉的错误多少也令人同情,因为埃尔基斯用计算机求得了㉑的第一组解是: $x=2682440$, $y=15365639$, $z=18796760$, $t=20615673$. 这些数虽然说不上惊人,但也大得难以验算.

上面提到的椭圆曲线是三次曲线, 与中学里学的椭圆截然不同. 椭圆曲线和三次不定方程有紧密的联系, 它是现代数学中一个充满活力的领域. 下面要说的另一个古老的问题现在发现也和椭圆曲线有关.

在第八节例 10 中曾提及边长为有理数的直角三角形. 我们简称为有理三角形,一个有趣的古老问题是:

对怎样的正整数 n，至少存在一个有理三角形，其面积恰为 n。

这样的 n，我们称之为合同数。下面先介绍几个关于合同数的结果。

例 11 完全平方数不能是合同数。

证明 假设对某个正整数 k，存在有理三角形其面积为 k^2，作一相似变换使各边成为整数(参考第八节例 10)，则面积为完全平方数，与第九节例 2 的结论矛盾。证毕。

同样，由于勾股三角形的面积不可能是平方数的两倍，所以 $2k^2(k\geqslant1)$ 也不是合同数。这样，1, 2, 4, 8, 9 都不是合同数。用较为困难的方法能够证明 3 不是合同数，但 5 却是合同数，例如边长为 $1\dfrac{1}{2}$，$6\dfrac{2}{3}$，$6\dfrac{5}{6}$ 的直角三角形的面积为 5。此外，6 显然是合同数。

由唯一分解定理易知，任何正整数 n 可以唯一地写成 q^2r 的形式。这里 $r\geqslant1$ 无平方因数（即不被任何素数的平方整除）。所以只需考虑无平方因数的合同数(否则作一个相似变换便化为这种情形)。

虽然我们所知的(无平方因数的)合同数还不多，但却可以证明下面的有趣结果：

例 12 设 n 是合同数，则有无穷多个(互不全等)有理三角形，它们的面积都是 n。

证明 可设 n 无平方因数，对面积为 n 的有理三角形作一相似变换，使之变为面积是 nd^2 的本原勾股三角形。这里 d 为一个正整数。

由第八节例 9 的注可知，存在任意多个互不全等的勾股三角形，面积均为 nd^2(d 是一个正整数)。对这些三角形作相

似比为 $\frac{1}{d}$ 的相似变换，即知存在任意多个有理三角形，互不全等，而面积都等于 n. 于是具有所说性质的有理三角形有无穷多个. 证毕.

在上面的证明中我们提到了，如果无平方因数 n 是合同数，则必有一个本原勾股三角形其面积为 nt^2（t 是某个整数）. 由此便得到了求合同数的一个"算法"：把所有本原勾股三角形的面积按从小到大次序排列，并将它们都分解成平方数与无平方因数的积，这得出了一个无平方因数的数列（注意，它不是单调递增的），此即全体（无平方因数的）合同数. 但是，这个算法远远不能令人满意. 首先，假如 n 是合同数，n 必然在上述数列中出现，但我们无法知道它何时才能出现；更重要的是这个算法并不能断言某个 n 不是合同数. 人们关心的是所谓的"实效算法"，即对每个给定的无平方因数 n，能够经过有限步的运算来判断它是否为合同数. 后面要说的突耐尔(Tunnell) 定理便是这方面的重要工作，在此之前请先看下面的例子.

例 13 n 为合同数的充分必要条件是存在 x，使得 x，$x+n$，$x-n$ 都是有理数的平方.

证明 面积为 n 的有理三角形 (a, b, c) $(a<b<c)$ 对应一个符合要求的 x，因为从

$$a^2+b^2=c^2, \ \frac{1}{2}ab=n$$

得出

$$(a\pm b)^2=c^2\pm 4n,$$

即

$$\left(\frac{a\pm b}{2}\right)^2=\left(\frac{c}{2}\right)^2\pm n,$$

于是取 $x=\left(\frac{c}{2}\right)^2$，则 x，$x+n$，$x-n$ 都是有理数的平方.

反过来，问题中说的 x 也对应一个面积为 n 的有理三角形. 因为若 x, $x+n$, $x-n$ 都是有理数的平方. 则

$$a=\sqrt{x+n}-\sqrt{x-n},\ b=\sqrt{x+n}+\sqrt{x-n},\ c=2\sqrt{x}$$

都是有理数，且满足

$$a<b<c,\ a^2+b^2=c^2,\ \frac{1}{2}ab=n.$$

此外，如果两直角三角形的面积及斜边对应相等，则它们全等. 故面积为 n 的不同的有理三角形(按上述方式)对应不同的 x. 所说的对应是一一对应. 证毕.

若设
$$x=\left(\frac{u}{v}\right)^2,\ x+n=\left(\frac{t}{v}\right)^2,$$
$$x-n=\left(\frac{w}{v}\right)^2$$

(t, u, v, w 都是正整数)，则例 13 中的条件等价于方程组

$$\begin{cases} u^2+nv^2=t^2, \\ u^2-nv^2=w^2 \end{cases} \tag{22}$$

有正整数解(u, v, t, w).

这个结论虽然很漂亮，但对于给定的 n，要判断方程组(22)是否有解仍很困难. 下面我们来推导合同数的另一个等价条件.

设边长为 a, b, c 的有理三角形的面积为 n，则

$$\left(\frac{a\pm b}{2}\right)^2=\left(\frac{c}{2}\right)^2\pm n,$$

将这两个等式相乘得到

$$\left(\frac{a^2-b^2}{4}\right)^2=\left(\frac{c}{2}\right)^4-n^2,$$

这表明方程 $u^4-n^2=v^2$ 有一组有理数解，即

$$u=\frac{c}{2},\ v=\frac{a^2-b^2}{4}.$$

用 u^2 同乘方程两边，就有

$$u^6-n^2u^2=(uv)^2.$$

取　　$$x=u^2=\left(\frac{c}{2}\right)^2,\ \ y=uv=\frac{1}{8}(a^2-b^2)c,$$

便给出三次方程

$$y^2=x^3-n^2x$$

的一组有理数解 (x, y).

换个说法，给定面积为 n 的有理三角形 (a, b, c)，我们(在 xOy 坐标系中)便得到椭圆曲线 $y^2=x^3-n^2x$ 上的一个有理点 (x, y)，其中

$$x=\left(\frac{c}{2}\right)^2.$$

反过来，曲线上的任一有理点是否必然可按上述方式产生呢？显然不是，如果设 (x, y) 是这样的一个有理点，则首先

$$x=\left(\frac{c}{2}\right)^2$$

必须是有理数的平方．此外，x 的分母应被 2 整除．这样，我们得到了曲线 $y^2=x^3-n^2x$ 上有理点 (x, y) 从一个(面积为 n 的)有理三角形产生的必要条件为：x 是有理数的平方且它的分母被 2 整除．例 14 表明这个条件也是充分的．

例 14　设 (x, y) 是曲线 $y^2=x^3-n^2x$ 上的一个有理点，假定 x 是有理数的平方且分母为偶数，那么，存在一个面积为 n 的有理三角形(按上述方式)对应于 x.

证明　设 $x=u^2$ (u 是正有理数)，令

$$v=\frac{y}{u},$$

则　　$$v^2=\frac{y^2}{x}=x^2-n^2,$$

即

$$v^2+n^2=x^2.\qquad ㉓$$

设 t 是 u 的分母(使 tu 为整数的最小正整数), 由假设 t 是偶数. 从 n 为整数及㉓易知 x^2, v^2 的分母相同, 即都是 t^4. 从而 $(t^2v)^2+(t^2n)^2=(t^2x)^2$, (t^2v, t^2n, t^2x) 是一组本原的勾股数. 由第八节定理可知, 存在整数 $p>q>0$, 使得

$$t^2v=p^2-q^2,\ t^2n=2pq,\ t^2x=p^2+q^2.$$

所以边长为 $\quad a=\frac{2p}{t},\ b=\frac{2q}{t},\ c=2u$

的直角三角形的面积是

$$\frac{2pq}{t^2}=n.$$

此外, 显而易见

$$x=u^2=\left(\frac{c}{2}\right)^2.$$ 证毕.

因此, n 是否为合同数, 就等价于椭圆曲线

$$E_n:\ y^2=x^3-n^2x$$

是否有理点(x,y), 使得 x 是有理数的平方且分母为偶数.

用椭圆曲线的理论可以证明(非常困难), 素数 $p\equiv5, 7 \pmod 8$ 都是合同数, 素数 $p\equiv3 \pmod 8$ 都不是合同数. 1983年突耐尔建立了下面的定理, 揭示出合同数与椭圆曲线之间的深刻联系.

定理 设正整数 n 无平方因数. 由

(i) n 是合同数

可以推出

(ii) 如果 n 是奇数, 方程 $n=2x^2+y^2+8z^2$ 的整数解数等于方程 $n=2x^2+y^2+32z^2$ 整数解数的两倍;

如果 n 是偶数, 方程 $n/2=4x^2+y^2+8z^2$ 的整数解数等于

方程 $n/2=4x^2+y^2+32z^2$ 整数解数的两倍.

反过来,如果关于椭圆曲线 E_n: $y^2=x^3-n^2x$ 的所谓 BSD 猜想是正确的话,则由(ii)也能推出(i).

请注意,对于给定的 n,(ii)中的方程都至多只有有限组整数解 (x, y, z),因此能够确定它们的解数. 这样我们便有了一个通过有限步的运算来判断 n 是否为合同数的算法. 遗憾的是这个算法依赖于一个尚未证明的猜想,所以问题还没有完全解决. 尽管如此,突耐尔给合同数这个古老问题注进了新鲜的血液. 这再一次表明,椭圆曲线这个充满了结果、猜想的现代数学领域是多么的重要和有力.

习 题

1．设 a, b 是给定的整数，$ab\neq 0$．如果方程 $ax+by=c$ 除了有限个整数 c 之外都有整数解 x, y，则 $(a, b)=1$．

2．掷硬币，得正面记 a 分，得背面记 b 分(a, b 都是正整数，且 $a>b$)．并将每次得分进行累计，如果有且仅有 35 个数永远不在记录上出现，58 就是其中之一，试确定 a, b．

3．设 $(a, b, c)=1$, $(a, b)=d$, $a=da_1$, $b=db_1$，则不定方程

$$ax+by+cz=n \quad ①$$

的全部解可表示成为

$$x=x_0+b_1t_1-u_1ct_2,\ y=y_0-a_1t_1-u_2ct_2,\ z=z_0+dt_2, \quad ②$$

其中 (x_0, y_0, z_0) 是①的一组特解，u_1, u_2 满足 $a_1u_1+b_1u_2=1$，t_1, t_2 是任意整数．

4．证明方程 $x+2y+3z=n$ 的非负整数解 (x, y, z) 的个数 $f(n)$ 由

$$f(0)=f(1)=1,\ f(2)=2,$$

$$f(n)=f(n-3)+\left[\frac{n}{2}\right]+1 \quad (n\geqslant 3)$$

给出．

5．求方程 $n^2+(n+1)^2=m^4+(m+1)^4$ 的全部整数解 (m, n)．

6．求方程 $a^b=b^a$ 的全部正整数解 $(a>b)$．

7．求方程 $|p^r-q^s|=1$ 的所有整数解．其中 p, q 为素数，r, s 为大于 1 的正整数．

8．设 $m>0$, $n>0$, 证明

$$\frac{m}{n}=\frac{1}{x}+\frac{1}{y}$$

有正整数解 (x,y) 的充分必要条件是存在正整数 a,b 满足 $a|n$, $b|n$, $m|a+b$.

9．设 p 是奇素数，则 2^p+3^p 不会是整数的 k 次方幂 $(k>1)$.

10．设 $n>2$, 则方程 $x^n+(x+1)^n=(x+2)^n$ 没有正整数解.

11．求方程 $3^n+4^n+\cdots+(n+2)^n=(n+3)^n$ 的全部正整数解.

12．设 a, b, c, d 都是奇数，$0<a<b<c<d$, $ad=bc$, 且 $a+d=2^k$, $b+c=2^m$, 则 $a=1$, $b=2^{m-1}-1$, $k=2(m-1)$.

13．求出所有大于 1 的整数 m, n, k, 使得

$$1!+2!+\cdots+m!=n^k.$$

14．求所有正整数 n, k, 使得 $(n-1)!=n^k-1$.

15．证明：连续四个正整数之积不是完全平方数．连续五个正整数的积也不会是完全平方数.

16．数论中的车比雪夫定理断言：若实数 $x>1$, 则有一个素数满足 $x<p<2x$. 应用这个结论证明：对 $n>1$, $k>1$, 方程 $n!=m^k$ 无解.

17．求出所有的边长为整数，周长是面积(数值)两倍的三角形.

18．求出方程 $5^x=2^y+3^z$ 的全部正整数解.

19．设 p 是素数，$n\geqslant 1$, 则方程 $x(x+1)=p^{2n}y(y+1)$ 没有正整数解 (x,y).

20．证明有无穷多个整数 n, 使方程 $x^4+y^4-z^4=n$ 没有

整数解(x, y, z).

21. 证明有无穷多个正整数的三数组(x^2, y^3, z^4)，使x^2, y^3, z^4成等差数列.

22. 证明方程$x^2+y^2+z^2+w^2=xyzw$有无穷多组正整数解.

23. 证明方程$x_1^2+x_2^2+\cdots+x_{29}^2=29x_1x_2\cdots x_{29}$有无穷多组正整数解$(x_1, x_2, \cdots, x_{29})$.

24. 设a, b, c都是整数，$a>0, b>0, c<0$. 如果方程$ax^2+by^2+cz^2=-abc$有整数解，则方程$ax^2+by^2+cz^2=0$有一组不全为0的整数解.

25. 设a, b, c都是整数，$abc\neq0$，且方程

$$ax^2+by^2+cz^2=0$$

有一组不全为0的整数解(x, y, z)，则

$$ax^2+by^2+cz^2=1$$

有一组有理数解.

26. 证明方程$(x-1)^2+x^2+(x+1)^2=y^2+(y+1)^2$有无穷多组正整数解$(x, y)$.

27. 证明数列$[n\sqrt{2}]$ $(n\geq1)$中有无穷多个完全平方数. 这里$[x]$表示实数x的整数部分.

28. 设$p\equiv1 \pmod 4$为素数，则方程$x^2-py^2=-1$有正整数解(x, y). 而当$p\equiv3 \pmod 4$时方程无解.

29. 证明方程$x^2+y^2=2(x+y)z+z^2$只有平凡整数解$(0, 0, 0)$.

30. 证明方程$a^2+b^2+c^2=a^2b^2$只有平凡整数解.

31. 求方程$x^3+y^3+z^3+x^2y+y^2z+z^2x+xyz=0$的全部整数解.

32. 证明方程$2x^2-5y^2=7^n$ $(n>0)$无整数解(x, y).

33. 证明方程 $x^4+y^4=3z^4$ 以及方程 $x^4+y^4=5z^4$ 都只有平凡整数解.

34. 设 p 是给定的素数，证明方程 $x^3+py^3+p^2z^3=0$ 只有平凡整数解.

35. 用无穷递降法证明方程 $x^4-y^4=z^2$ 没有 $z\neq0$ 的整数解.

36. 用第九节例 4 的结论来证明勾股三角形的面积不会是完全平方.

37. 证明 $(5\times2^k)^2(k\geqslant0)$ 不能表示成三个正整数的平方和.

38. 证明整数 1, 3, 5, 9, 11, 17, 29, 41, 2×4^k, 6×4^k, $14\times4^k(k\geqslant0)$ 都不能表示成四个正整数的平方和.

39. 一群年轻人去跳舞，每跳一次舞需交 1 元钱. 每个男孩与每个女孩恰好跳了一次后，大家去另一处跳舞，这里用辅币支付，他们用了与前面同样多的钱. 每个人的入场费是 1 辅币，每人跳一次舞需交 1 辅币，并且每个人恰好与其他人各跳两次舞(不分性别). 最后还剩下 1 个辅币. 问 1 元钱兑换多少辅币.

40. 求出所有正整数 x, y, 使得 $y|x^2+1$, $x|y^2+1$.

习题解答概要

1．如果$(a, b)>1$，因(a, b)的素因子只有有限个，这样，只要取c为异于(a, b)的素因子的素数(有无穷多个！因为素数的个数无限)，则$(a, b)\nmid c$，所以对这样的c，方程$ax+by=c$都无整数解，与已知条件矛盾．故$(a, b)=1$．

2．一个正整数n可记录，意味着$n=ax+by$有非负整数解(x,y)，首先必有$(a, b)=1$，否则有无穷多个n不能被记录(习题1)，与已知条件不符．再由所给条件及第一节例11可知

$$\frac{1}{2}(a-1)(b-1)=35.$$

根据$a>b$，$(a, b)=1$，易知$(a, b)=(71, 2)$或$(11, 8)$．但是

$$71\times 0+2\times 29=58,$$

所以$(a, b)=(71, 2)$不合要求．又易验证，当$a=11$，$b=8$时，58不被记录．故所求的解是$(a, b)=(11, 8)$．

3．不难验证，由(2)确定的(x, y, z)是(1)的整数解．

反过来，设x, y, z是(1)的任一组解，由

$$ax_0+by_0+cz_0=n, \quad ax+by+cz=n$$

可得
$$d[a_1(x-x_0)+b_1(y-y_0)]=-c(z-z_0),$$

因$(d, c)=1$，故有整数t_2，使得$z=z_0+dt_2$，代入上式得

$$a_1(x-x_0)+b_1(y-y_0)=-ct_2, \qquad ③$$

由于$X=-u_0ct_2$，$Y=-v_0ct_2$是方程$a_1X+b_1Y=-ct_2$的一组解，这样，由$(a_1, b_1)=1$并用第一节定理2，从而推出，存在整数t_1使得

$$x-x_0=b_1t_1-u_0ct_2, \quad y-y_0=a_1t_1-v_0ct_2.$$

4．归纳法．显然$f(0)=f(1)=1$，$f(2)=2$．设$n\geqslant 3$，将方程

$$x+2y+3z=n$$

的非负解分成不交的两组：(x, y, z)，$z\geqslant 1$；以及(x, y, z)，$z=0$．

对于$z\geqslant 1$，方程化为$x+2y+3(z-1)=n-3$．由归纳假设，解数

是 $f(n-3)$.

当 $z=0$ 时，方程为 $x+2y=n$，易见所求解数是 $\left[\frac{n}{2}\right]+1$. 故

$$f(n)=f(n-3)+\left[\frac{n}{2}\right]+1$$

(比较第一节例 15).

5. 方程化为 $n(n+1)=m(m+1)(m^2+m+2)$，设 $k=m^2+m$，则有 $n(n+1)=k(k+2)$，配方成为 $(2k+2)^2-(2n+1)^2=3$，由此易得 $(m, n)=(0, 0)$, $(0, -1)$, $(-1, 0)$, $(-1, -1)$.

6. 设 $(a, b)=d$, $a=a_1d$, $b=b_1d$, 则 $(a_1, b_1)=1$, $a_1>b_1$, 方程化为

$$a_1^{b_1}=b_1^{a_1}d^{a_1-b_1},$$

于是 $b_1^{a_1}|a_1^{b_1}$，因 $(a_1, b_1)=1$，故 $b_1=1$，所以 $a_1=d^{a_1-1}$. 显然 $d\neq1$，从而有 $a_1\geqslant2^{a_1-1}\geqslant(a_1-1)+1=a_1$，故 $d=2$, $a_1=2$，这样 $a=4$, $b=2$.

7. 由于 p, q 都是素数，由 $|p^r-q^s|=1$ 可知 p, q 中有一个是 2. 不妨设 $q=2$，则方程为

$$p^r=2^s+1 \quad 或 \quad p^r=2^s-1,$$

应用第三节例 7 及例 8 即得所有的解.

8. 充分性显而易见.

必要性：如果

$$\frac{m}{n}=\frac{1}{x}+\frac{1}{y}=\frac{x+y}{xy},\ x>0,\ y>0,$$

设 $$(x, y)=d,\ (m, n)=l,$$

则有 $x=dx_1$, $y=dy_1$, $(x_1, y_1)=1$, $m=lm_1$, $n=ln_1$, $(m_1, n_1)=1$,

于是 $$\frac{m_1}{n_1}=\frac{x_1+y_1}{dx_1y_1},$$

即 $$m_1dx_1y_1=n_1(x_1+y_1).$$

由于 $(x_1, y_1)=1$，故 $(x_1y_1, x_1+y_1)=1$，从上式得

$$x_1y_1|n_1,\ m_1|x_1+y_1,$$

取 $a=lx_1$, $b=ly_1$，则有 $lx_1y_1|n_1l$, $lm_1|lx_1+ly_1$，即 $a|n$, $b|n$, $m|a+b$.

9. $p=5$ 时结论显然. 当 $p\neq5$ 时，易知 $2^p+3^p\equiv0 \pmod 5$. 但当 $p\neq5$ 时，$2^p+3^p=2^p+(5-2)^p\equiv5p\times2^{p-1}\not\equiv0 \pmod{5^2}$，故 2^p+3^p 不能是整数的 k 次方幂 $(k>1)$.

10．模 $x+1$ 得，$(-1)^n\equiv 1(\bmod x+1)$，故 n 是偶数．记 $y=x+1$，我们有

$$y^n=2C_n^1y^{n-1}+\cdots+2C_n^{n-1}y\quad(n\geqslant 4).$$

由此可见 $y^n>2ny^{n-1}$，即 $y>2n$．但从上式又得出 $y\mid 2n$，即 $y\leqslant 2n$，矛盾．

11．$n=2,3$ 是解．$n=1,4,5$ 均不是解．对于 $n\geqslant 6$，用归纳法可证明

$$3^n+4^n+\cdots+(n+2)^n<(n+3)^n.$$

如果这不等式对 n 已成立($n\geqslant 6$)，则对 $n+1$ 时，

$$\begin{aligned}&3^{n+1}+4^{n+1}+\cdots+(n+3)^{n+1}\\&<(n+3)(3^n+4^n+\cdots+(n+2)^n)+(n+3)^{n+1}\\&<2(n+3)^{n+1}=(n+4)^{n+1}\times 2\left(\frac{n+3}{n+4}\right)^{n+1}\\&<(n+4)^{n+1}.\end{aligned}$$

12．由 $a+d=2^k$，$b+c=2^m$，得 $d=2^k-a$，$c=2^m-b$，代入 $ad=bc$ 中，有 $a(2^k-a)=b(2^m-b)$，即

$$b\cdot 2^m-a\cdot 2^k=b^2-a^2. \qquad ①$$

易知 $k>m\geqslant 3$．由①得出

$$2^m(b-a\cdot 2^{k-m})=(b+a)(b-a), \qquad ②$$

因 a，b 都是奇数，故 $a+b$，$a-b$ 都是偶数，又易见它们不能都被4整除．由于

$$b-a<b<\frac{1}{2}(b+c)=2^{m-1},\ b+a<b+c=2^m,$$

从②可知

$$\begin{cases}b+a=2^{m-1},\\ b-a=2(b-a\cdot 2^{k-m}).\end{cases}$$

由第二个式子得 $b+a=2^{k+1-m}a$，即 $2^{m-1}=2^{k+1-m}a$，所以奇数 $a=1$，及 $b=2^{m-1}-1$，$k=2(m-1)$．

13．先证明当 $m\geqslant 8$ 时，必有 $k=2$．因为

$$1!+2!+\cdots+6!\equiv 9(\bmod 27),$$

$$7!+8!+\cdots+m!\equiv 0(\bmod 27),$$

故当 $m\geqslant 8$ 时，$1!+2!+\cdots+m!$ 被 3^2 整除，但不能被 3^3 整除，所以必

有 $k=2$，再由第五节例 10 可知此时无解．当 $m<8$ 时，易检验得出所有解是 $(m,n,k)=(3,3,2)$．

14．当 $n\leqslant 5$ 时易求得解是 $(n,k)=(2,1),(3,1),(5,2)$．当 $n>5$ 时，显然 n 是奇数，且

$$2<\frac{n-1}{2}<n-3,$$

故 2 及 $\frac{n-1}{2}$ 出现在 $(n-2)!$ 中，从而 $(n-1)\mid(n-2)!$，我们又有

$$\begin{aligned}(n-1)(n-2)! &= n^k-1=((n-1)+1)^k-1\\ &=(n-1)^k+C_k^1(n-1)^{k-1}+\cdots\\ &\quad+C_k^{k-2}(n-1)^2+k(n-1),\end{aligned}$$

故 $(n-1)\mid k$，于是 $k\geqslant n-1$，从而 $n^k-1\geqslant n^{n-1}-1>(n-1)!$，所以方程没有 $n>5$ 的解．

15．设 $x(x+1)(x+2)(x+3)=y^2$，$x>0$，则有

$$(x^2+3x+1)^2-y^2=1,$$

这不可能．

若有 $x(x+1)(x+2)(x+3)(x+4)=y^2$，$x>0$，当 x 为奇数时，易证 $x+2$ 与 $x(x+1)(x+3)(x+4)$ 互素．故 $x(x+1)(x+3)(x+4)$ 为完全平方，但

$$((x^2+4x)+1)^2<x(x+1)(x+3)(x+4)<((x^2+4x)+2)^2,$$

矛盾．

当 x 为偶数时，先考虑 $x\equiv 0,4\pmod 6$ 的情形．此时 $x+1$ 与 $x(x+2)(x+3)(x+4)$ 互素，故这两数均是完全平方，但

$$\left(x^2+\frac{9}{2}x+2\right)^2<x(x+2)(x+3)(x+4)<\left(x^2+\frac{9}{2}x+3\right)^2.$$

若 $x\equiv 2\pmod 6$，则 $x+3$ 与 $x(x+1)(x+2)(x+4)$ 互素．所以这两数都应是完全平方．然而当 $x\neq 2$ 时，有

$$\left(x^2+\frac{7}{2}x\right)^2<x(x+1)(x+2)(x+4)<\left(x^2+\frac{7}{2}x+1\right)^2$$

导出矛盾．又 $x=2$ 显然不是解．

16．$n=2$ 时结论显然．设 $n>2$，则由车比雪夫定理可知，存在一个素数 p，使得

$$\frac{n}{2}<p\leqslant n.$$

在1, 2, …, n中只有一个数被p整除(即p自身)，所以$n!$中p的方幂为1，由此易见$n!\neq m^k(k>1)$.

17. 设三角形的边长为整数a, b, $c(0<a\leqslant b\leqslant c)$，$p$为半周长，则

$$p^2=p(p-a)(p-b)(p-c).$$

于是 $$4(a+b+c)=(a+b-c)(a+c-b)(b+c-a).$$

上式右边三个因数的奇偶性相同，左边是偶数，所以右边的因数都是偶数。

令 $x=\frac{1}{2}(b+c-a)$, $y=\frac{1}{2}(a+c-b)$, $z=\frac{1}{2}(a+b-c)$,

则$x\geqslant y\geqslant z$，且$x+y+z=xyz$，由此得知$yz\leqslant 3$，这样不难求出$x=3$, $y=2$, $z=1$，即$a=3$, $b=4$, $c=5$.

18. 模3，由于$5\equiv 2\equiv -1(\bmod 3)$，故$(-1)^x\equiv(-1)^y(\bmod 3)$，所以$x$, y同奇偶性.

当x, y都是偶数时，设$x=2x_1$，则有

$$2^y+3^z=(5^{x_1})^2,$$

由第五节例12可知，解为$y=4$, $z=2$, $x_1=1$.

当x, y都是奇数时，设$x=2x_1+1$，如果$y>1$，则$y\geqslant 3$，模8，因$8|2^y$, $5^x=(5^2)^{x_1}\cdot 5\equiv 5(\bmod 8)$，故$3^z\equiv 5(\bmod 8)$. 但按$z$为奇、偶数，$3^z$模8分别是3和1，这就导出矛盾，于是$y=1$，方程化为

$$5^x-3^z=2,$$

由第七节例4可知其解为$x=1$, $z=1$. 因此所求的解为

$$(x, y, z)=(1, 1, 1), (2, 4, 2).$$

19. 设$k=p^n(n\geqslant 1)$. 如果有正整数x, y使得

$$x(x+1)=k^2y(y+1),$$

易知$x>ky$，设

$$x=ky+b(b\geqslant 1),$$

代入上式得到

$$b(b+1)=k[k-(2b+1)]y$$

所以$k|b(b+1)$. 但$(b, b+1)=1$，而k是素数的方幂，故$k|b$或者$k|(b+1)$，这与$k>2b+1$矛盾.

20. 取 $n\equiv 3(\bmod 5)$ 即可，请比较第六节例 2.

21. 方程 $x^2+z^4=2y^3$ 有一组正整数解 $x=13$, $y=5$, $z=3$，故有无穷多组解 $x=13d^6$, $y=5d^4$, $z=3d^3(d\geqslant 1)$.

22. $x=y=z=w=2$ 是解. 此外，如果 (x, y, z, w) 是正整数解，则 $(x, y, z, xyz-w)$ 也是正整数解，故解数无穷.

23. $x_1=x_2=\cdots=x_{29}=1$ 是解. 如果 $(x_1, x_2, \cdots, x_{29})$ 是一组正整数解，则 $(x_1, x_2, \cdots, x_{28}, 29x_1\cdots x_{28}-x_{29})$ 也是正整数解.

24. 从 $ax^2+by^2=-c(z^2+ab)$，得

$$(ax^2+by^2)(z^2+ab)=-c(z^2+ab)^2,$$

即
$$a(xz+by)^2+b(yz-ax)^2=-c(z^2+ab)^2.$$

因为 $ab>0$，故 $z^2+ab\neq 0$. 这就得到了一组不全为 0 的整数解.

25. 设整数 α, β, γ 满足 $a\alpha^2+b\beta^2+c\gamma^2=0(\alpha\neq 0)$. 令

$$x=\alpha(1+t),\ y=\beta(1-t),\ z=\gamma(1-t),$$

则
$$ax^2+by^2+cz^2=2t(a\alpha^2-b\beta^2-c\gamma^2)=4t\cdot a\alpha^2,$$

取
$$t=\frac{1}{4a\alpha^2},$$

则得出 $ax^2+by^2+cz^2=1$ 的一组有理数解.

26. 原方程即 $6x^2+3=(2y+1)^2$，所以 $3\mid(2y+1)$，令 $2y+1=3u$，则有 $3u^2-2x^2=1$. 令 $a=3u-2x$, $b=x-u$，则方程成为 $a^2-6b^2=1$. 参考第七节例 7. 我们实际上求出了全部的解 (x, y).

27. 由第七节可知，有无穷对正整数 u, v，使得

$$u^2-2v^2=-1,$$

故
$$2u^2v^2=u^4+1,$$

所以 $u^2<\sqrt{2}uv<u^2+1$，即 $[\sqrt{2}uv]=u^2$.

28. 由第七节定理 1，方程 $x^2-py^2=1$ 有正整数解，模 4 可知 $2\nmid x$, $2\mid y$. 设 (x_1, y_1) 为其最小解. 我们有

$$\frac{x_1-1}{2}\cdot\frac{x_1+1}{2}=\frac{x_1^2-1}{4}=\frac{py_1^2}{4}=p\left(\frac{y_1}{2}\right)^2,$$

于是存在正整数 u, v 使得

$$\frac{x_1-1}{2}=pu^2,\ \frac{x_1+1}{2}=v^2,\ y_1=2uv, \qquad ①$$

或者

$$\frac{x_1-1}{2}=u^2,\quad \frac{x_1+1}{2}=pv^2,\ y_1=2uv \qquad ②$$

如果①成立，则

$$v^2-pu^2=1,$$

但

$$u=\frac{y_1}{2v}<y_1,$$

与(x_1, y_1)是最小解矛盾。

因此②必须成立，即得出

$$u^2-pv^2=-1,$$

所以方程 $x^2-py^2=-1$ 有解 $x=u,\ y=v$。

当 $p\equiv 3 \pmod 4$ 时，模 4 即知 $x^2-py^2=-1$ 无解。

29．设 $t=x+y+z$，则 $2x^2+2xy+2y^2=t^2$，故 $2|t$，设 $t=2t_1$，则

$$x^2+xy+y^2=2t_1^2,$$

$x,\ y$ 必须都是偶数，设 $x=2x_1,\ y=2y_1$，得

$$2x_1^2+2x_1y_1+2y_1^2=t_1^2.$$

重复上面论证，可见 $x,\ y$ 被 2 的任意高次幂整除，从而 $x=y=0$，于是 $z=0$，参考第五节例 17。

30．模 4 可证明 $a,\ b,\ c$ 都是偶数，重复这个论证得知必须 $a=b=c=0$。

31．$x,\ y,\ z$ 不能都是奇数，不能两奇一偶，也不能两偶一奇，所以它们都是偶数。方程两边约去 2^2，再重复这个论证，推出 $x=y=z=0$。

32．取使方程有解的最小的 n，模 7 可知方程

$$2x^2-5y^2=7^{n-2}$$

也有解，与 n 的选择矛盾。

33．分别模 3 及模 5，参考第五节例 15。

34．参考第五节例 15。

35．设有正整数解(x, y, z)，$x\neq y$，我们选择使 x 最小的一组。与第九节例 5 一样地可证明此时有$(x, y)=1$。又易见 x 是奇数。

当 $2|y$ 时，应用第八节中定理可求得整数 $a>b>0$，使得

$$x^2=a^2+b^2,\ y^2=a^2-b^2,$$

故 $a^4-b^4=(xy)^2$，这得出方程的一组正整数解(a, b, xy)，但 $0<a<x$，与 x 的最小性矛盾。

当 $2|y$ 时，同理有整数 $a>b>0$，$(a, b)=1$，a，b 一奇一偶，使得

$$x^2=a^2+b^2,\ y^2=2ab,$$

不妨设 a 为偶数，则从 $y^2=2ab$ 推出 $a=2p^2$，$b=q^2$，p，q 都是整数，且 $2\nmid q$，$(p, q)=1$。于是

$$x^2=(2p^2)^2+q^2,$$

从而又有整数 $r>s>0$，$(r, s)=1$，使得

$$2p^2=2rs,\ q^2=r^2-s^2,$$

因 $(r, s)=1$，故由 $p^2=rs$ 得知 $r=m^2$，$s=n^2$，这样

$$m^4-n^4=q^2,$$

但 $0<m=\sqrt{r}\leqslant p<x$，矛盾。

36．设勾股三角形 (a, b, c) 的面积为 d^2，则

$$a^2+b^2=c^2,\ ab=2d^2.$$

设 $a>b$，则 $c^2+(2d)^2=(a+b)^2$，$c^2-(2d)^2=(a-b)^2$，与第九节例 4 矛盾。

37．5^2 不能表示成三个正整数的平方和，用第五节例 18 的方法即知 $(5\times 2^k)^2(k\geqslant 0)$ 不能表示成三个正整数的平方和。

38．参考习题 37．

39．设有 b 个男孩，g 个女孩，又设 1 元钱可兑换 x 个辅币，则起先共跳 bg 次舞，后来共跳 $2C_{b+g}^2=(b+g)(b+g-1)$ 次舞。由题意得到

$$bgx=(b+g)(b+g-1)+(b+g)+1,$$

即

$$(b+g)^2+1=bgx.$$

令 $z=x-2$，则有

$$g^2+b^2+1=bgz.$$

由第九节例 8 可知，必须 $z=3$，即 $x=5$。

40．设 $x|y^2+1$，$y|x^2+1$，则 x，y 互素并且 x^2+y^2+1 分别被 x，y 整除，从而 x^2+y^2+1 被 xy 整除，即有整数 z 使得

$$x^2+y^2+1=xyz,$$

由第九节例 8 可知，必须 $z=3$，而方程 $x^2+y^2+1=3xy$ 的全部正整数解已由第九节例 9 求出。

附　录

整数的基本知识

(一) 整　除

1. 任意给定两个整数 a, b, $b\neq 0$. 如果存在一个整数 q, 使得 $a=bq$, 则我们称 b 整除 a, 记作 $b|a$. 这时称 a 为 b 的倍数, 称 b 为 a 的约数(或因数). 如果不存在上述的整数 q, 则称 b 不整除 a, 记为 $b\nmid a$.

例如: $3|6$, $1|-7$, $4|0$, $-5|75$, $2\nmid 9$, $64\nmid 1989$.

2. (带余除法)设 a, b 是任意给定的两个整数, 其中 $b\neq 0$, 则存在整数 q 和 r, 使得

$$a=bq+r,\ 0\leqslant r<|b|.$$

这样的 q, r 是唯一的.

3. 设 a, b 是不全为 0 的整数, 如果非零整数 d 同时整除 a, b, 则称 d 为它们的公约数. 所有公约数中最大的称为 a, b 的最大公约数, 记为 (a, b). 注意, 如 d 是公约数, 则 $-d$ 也是. 所以最大公约数一定是正整数.

a, b 恒有公约数 ± 1. 如果这是仅有的公约数, 即

$$(a, b)=1,$$

则称 a, b 互素(或互质). 一般地, 设 $(a, b)=d$, 则可将 a, b 分解为 $a=a_1d$, $b=b_1d$, a_1, b_1 都是整数, 且 $(a_1, b_1)=1$.

例如: $(2, -7)=1$, $(3, 11)=1$, $(5, 35)=5$, $(0, -3)=3$.

类似地可定义 $k(>2)$ 个不全为 0 的整数 $a_1, a_2, \cdots, a_k$ 的最大公约数，即为它们所有公约数中的最大者，记为 $(a_1, a_2, \cdots, a_k)$. 当 $(a_1, a_2, \cdots, a_k)=1$ 时，称 $a_1, a_2, \cdots, a_k$ 互素. 请注意，$a_1, a_2, \cdots, a_k$ 互素不能推出它们两两互素（反过来当然正确）. 但其中任意 $k-1$ 个数的最大公约数必与第 k 个互素. 此外，设 $(a_1, a_2, \cdots, a_k)=d$，则 $a_1, a_2, \cdots, a_k$ 可分解成为 $a_1=da_1', a_2=da_2', \cdots, a_k=da_k'$，其中 $a_1', a_2', \cdots, a_k'$ 都是整数，且 $(a_1', a_2', \cdots, a_k')=1$.

例如：$(2, 4, -10)=2$, $(4, 0, 71, 8)=1$, $(6, 10, 15)=1$.

提醒一下，本书中常用有序数组 (x, y), (x, y, z) 等等来表示不定方程的整数解. 请读者结合上下文将它们与最大公约数的记号区分开.

4. 设 a, b 是两个正整数，如果 $a|c$, $b|c$，则称 c 是 a, b 的公倍数. 所有这些公倍数中的最小正数称为 a, b 的最小公倍数，记为 $[a, b]$. 对于 $k(>2)$ 个整数，也可类似地定义最小公倍数，但本书不需要这些.

例如：$[3, 6]=6$, $[5, 7]=35$, $[20, 36]=180$.

a, b 的最大公约数与最小公倍数满足如下关系式：

$$(a, b)[a, b]=ab.$$

5. 本书中所用到的整除性质和有关结论如下（字母均表示整数）：

(1) 若 $a|b$, $b|c$，则 $a|c$.

(2) 若 $a|b$, $b\neq 0$，则 $|b|\geqslant|a|$.

(3) 若 $a|bc$，且 $(a, c)=1$，则 $a|b$.

(4) 若 $a|b$, $a|c$，则 $a|(b+c)$, $a|(b-c)$；更一般地，我们有 $a|(bx+cy)$，其中 x, y 为任意整数.

(5) 若$a|b$, $a|c$, 则$a|(b, c)$.

(6) 若$a|c$, $b|c$, 则$[a, b]|c$. 特别地, 当$(a, b)=1$时, 有$ab|c$.

(7) $(a, b)=(a, b+ax)$, x是任意整数.

(8) 设$a>0$. 则$\sqrt{a}$为有理数的充分必要条件是a为完全平方数.

6. 大于1的整数, 如果它的正约数只有1和它自身, 则称它为素数(或质数), 否则称作合数.

例如: 2, 3, 5, 7, 11, 23是素数; 4, 6, 8, 9, 21是合数.

2是唯一的偶素数. 可以证明素数有无穷多个.

素数常用字母p表示, 其特性是:

如果$p|ab$, 则$p|a$, 或者$p|b$. 于是从$p|ab$, $p\nmid a$, 便推出$p|b$. 注意$p\nmid a$等价于说$(p, a)=1$.

7. (唯一分解定理)任一大于1的整数n能够唯一地写成

$n=p_1^{a_1}p_2^{a_2}\cdots p_k^{a_k}$, 其中 $a_i>0(1\leqslant i\leqslant k)$, $p_1<p_2<\cdots<p_k$ 为素数.

所谓唯一的意思是说, 如果还有$b_i>0(1\leqslant i\leqslant l)$及素数$q_1<q_2<\cdots<q_l$, 使得

$$n=q_1^{b_1}q_2^{b_2}\cdots q_l^{b_l},$$

则$k=l$, 并且

$$p_i=q_i, \ a_i=b_i(1\leqslant i\leqslant k).$$

这一定理也称为算术基本定理, 上述的分解式称为n的标准分解或者n的素因数分解. 对于小于-1的整数n也有类似的分解, 这只要注意$n=-(-n)$.

例如: $60=2^2\times3\times5$, $539=7^2\times11$, $-805=-5\times7\times23$.

由唯一分解定理容易推出如下结果（以下字母均表示整数）：

(1) 设 $a=p_1^{a_1}p_2^{a_2}\cdots p_l^{a_l}$，$a_i\geqslant0(1\leqslant i\leqslant l)$，$b=p_1^{b_1}p_2^{b_2}\cdots p_l^{b_l}$，$b_i\geqslant0(1\leqslant i\leqslant l)$，则

$$(a,b)=p_1^{\min(a_1,b_1)}p_2^{\min(a_2,b_2)}\cdots p_l^{\min(a_l,b_l)},$$

$$[a,b]=p_1^{\max(a_1,b_1)}p_2^{\max(a_2,b_2)}\cdots p_l^{\max(a_l,b_l)}.$$

这里 $\min(a_i,b_i)$ 表示 a_i，b_i 中的较小者，$\max(a_i,b_i)$ 表示 a_i，b_i 中的较大者.

(2) 若 $(a,b)=1$，则对任意正整数 k，有 $(a^k,b^k)=1$，反之亦然.

(3) 若正整数 n 是某个整数的 k 次方幂，则称 n 是 k 次方幂 $(k\geqslant2)$. 1 当然是 k 次方幂. 大于 1 的整数 n 是 k 次方幂的充分必要条件是，其标准分解中每个素数的指数都被 k 整除.

此外，设 m_1，m_2，…，m_l 都是正整数，两两互素，且 $m_1m_2\cdots m_l$ 为 k 次方幂 $(k>1)$，则 m_1，m_2，…，m_l 都是 k 次方幂. 这个结论本书中屡次用到.

（二）同　余

1. 设 $m\geqslant1$，任意整数被 m 除所得的余数有 m 种可能的值，即 0，1，…，$m-1$（见前面的带余除法）. 如果两个整数 a，b 被 m 除所得的余数相同，即 $m\mid(a-b)$，我们就称 a，b 模 m 同余，记为 $a\equiv b(\mathrm{mod}\,m)$. 如果 $m\nmid(a-b)$，则记为 $a\not\equiv b(\mathrm{mod}\,m)$.

例如： $10\equiv3(\mathrm{mod}\,7)$，$-5\equiv8(\mathrm{mod}\,13)$，

$$64\not\equiv0(\mathrm{mod}\,1989).$$

同余式有许多与等式类似的性质（以下字母均表示整

数)：

(1) $a\equiv a(\bmod m)$.

(2) 若 $a\equiv b(\bmod m)$，则 $b\equiv a(\bmod m)$.

(3) 若 $a\equiv b(\bmod m)$，$b\equiv c(\bmod m)$，则 $a\equiv c(\bmod m)$.

(4) 若 $a\equiv b(\bmod m)$，则 $ka\equiv kb(\bmod m)$.

(5) 若 $a_1\equiv b_1(\bmod m)$，$a_2\equiv b_2(\bmod m)$，则

$$a_1\pm a_2\equiv b_1\pm b_2(\bmod m).$$

(6) 若 $a_1\equiv b_1(\bmod m)$，$a_2\equiv b_2(\bmod m)$，则

$$a_1a_2\equiv b_1b_2(\bmod m).$$

(7) 若 $a\equiv b(\bmod m)$，则 $a^k\equiv b^k(\bmod m)$，其中 $k\geqslant 1$.

(8) 若 $an\equiv bn(\bmod m)$，则

$$a\equiv b\left(\bmod \frac{m}{(m,\ n)}\right);$$

当 $(m,\ n)=1$ 时，$a\equiv b(\bmod m)$.

2. 设 $m\geqslant 1$，我们可以依模 m 把全体整数分类，被 m 除得相同余数的归同一类，这样全体整数分成了 m 个类(任意两个类都无公共数)：

$$A_0,\ A_1,\ \cdots,\ A_{m-1},$$

其中 A_i 表示被 m 除后余数为 i 的所有整数 $(0\leqslant i\leqslant m-1)$，即

$$A_i=\{km+i,\ k\text{ 是任意整数}\}(0\leqslant i\leqslant m-1).$$

如果整数 a_i 取自 $A_i(0\leqslant i\leqslant m-1)$，则 $\{a_0,\ a_1,\ \cdots,\ a_{m-1}\}$ 称为模 m 的一组完全剩余系，我们经常把完全剩余系取为 $\{0,\ 1,\ \cdots,\ m-1\}$.